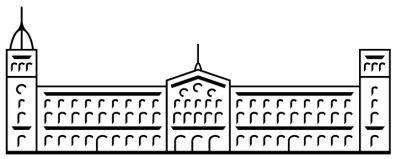


Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Sobre el principi local-global en Teoria de Nombres

Autor: Oriol Fernández Peña

Director: Dra. Núria Vila Oliva
Departament de Matemàtiques i Informàtica
Barcelona, 29 de juny de 2017

Abstract

The aim of this Bachelor's Thesis is to make an introduction of the local-global concept in Number Theory. In order to do this we construct the p-adic numbers in two different ways, we give some fundamental properties and we exhibit its structure. We present the Hilbert symbol in order to use it on the study of quadratic spaces and to determine which of them are isotropic and under which conditions. We use all the theory developed about quadratic spaces to finally formulate the Hasse-Minkowski theorem and we give a proof. In the last chapter, we show some counter-exemples of the Hasse principle, some of them classics and some others recently publicated.

Resum

L'objectiu d'aquest Treball Final de Grau és fer una introducció al concepte local-global en Teoria de Nombres. Per a això fem una construcció dels nombres p-àdics de dues formes diferents, en donem propietats fonamentals i mostrem la seva estructura. Presentem el símbol de Hilbert i l'aprofitem per poder arribar a l'estudi dels espais quadràtics i determinar quins són isotròpics i sota quines condicions. Utilitzem tota la teoria sobre espais quadràtics desenvolupada per a, finalment, enunciar el teorema de Hasse-Minkowski i donar-ne una prova. En l'últim capítol presentem alguns contraexemples clàssics i publicats recentment al principi de Hasse.

Agraïments

Vull agrair a la Dra. Núria Vila Oliva la guia que m'ha ofert durant el transcurs del semestre, els seus consells i interès; sobretot encoratjant-me a llegir i descobrir articles antics i recents per poder tenir una visió del tema la més àmplia possible.

Índex

Introducció

L'any 1920, Kurt Hensel (1861-1941) construí per primera vegada els nombres p-àdics. Ho feu mitjançant les distàncies ultramètriques que ell mateix definí sobre $\mathbb{Q}$. En aquest sentit dotà de llenguatge els estudis que anteriorment havia fet Hermann Minkowski (1964-1909) en que establia que sota unes certes condicions unes equacions tenien solució en $\mathbb{Q}$ si en tenien mòdul p^k per a tot p primer i tot $k \geq 1$. Pocs anys més tard, Hensel encarregà al seu estudiant de doctorat Helmut Hasse (1898-1979) ordenar i desenvolupar aquesta nova branca d'estudi. Finalment, Hasse generalitzà els resultats de Minkowski i demostrà el que avui coneixem com a teorema de Hasse-Minkowski, o Principi de Hasse.

Aquest teorema estableix que tot polinomi homogeni a coeficients enters té solució entera si, i només si, en té per a tot $\mathbb{Q}_p$. Del fet que els p-àdics $\mathbb{Q}_p$ són cossos locals donà el tret de sortida a l'estudi local-global i es conjecturà que el Principi de Hasse se sostenia per a equacions diofantines en general. L'any 1951, Ernst Selmer donà el primer contraexemple. Des de llavors s'ha estudiat profundament i han sigut trobats una immensa quantitat d'equacions que no satisfan el Principi de Hasse.

Alguns contraexemples proposats passen per generalitzacions de l'equació de Fermat. En aquest sentit es defineixen les corbes de Fermat C d'exponent p amb unes certes condicions. Alain Kraus i Henri Cohen, entre d'altres, proposen resultats que semblen factible que per a tot primer p existeixin infinites corbes de Fermat que contradiuen el Principi de Hasse, emperò aquest fet resta sense demostrar.

Estructura de la memòria

El treball es divideix en quatre capítols.

En el primer fem una construcció dels nombres p-àdics seguint el text de A. Robert [12] i en desenvolupem propietats importants dels cossos p-àdics a fi de poder posar llenguatge i poder demostrar el teorema principal de la memòria.

En el segon capítol tractem el símbol de Hilbert, que està íntimament lligat a l'estructura de les formes quadràtiques. Seguim els textos de Borevich-Shafarevich [3] i Serre [13]. Donem eines per a computar de manera local el símbol i en donem propietats

globals.

En el tercer capítol desenvolupem tota la teoria necessària d'espais quadràtics per finalment demostrar el Teorema de Hasse-Minkowski. En aquest capítol seguim el text de O.T. O'Meara [11] però adaptem les demostracions per evitar haver d'introduir conceptes innecessaris pel nostre objectiu fent així els resultats més clars i directes.

En el quart i últim capítol presentem el contraexemple de Selmer i seguim la demostració que dóna K. Conrad [6], exposem també un criteri per a uns sistemes d'equacions homogènies de grau 2 seguint l'article de W. Aitken i F Lemmermeyer [1], i finalment exposem uns resultats molt recents de A. Kraus i de H. Cohen [9] i [4].

Prerequisits

En la majoria de resultats de la memòria dels tres primers capítols no fem referència a resultats que no siguin bàsics, el nostre objectiu era escriure un text autocontingut en gran mesura i constructiu, és a dir, de definicions bàsiques arribar a resultats importants. Només fem servir nocions bàsiques que apareixen en assignatures del grau, en especial *Estructures Algebraiques* i *Equacions Algebraiques*.

En l'últim capítol fem servir tots els resultats obtinguts en l'assignatura *Mètodes algebraics en Teoria de Nombres* que poden ser trobats en el text de H. Cohen [4].

Capítol 1

Els nombres p-àdics

1.1 L'anell $\mathbb{Z}_p$

Definició 1.1.1. *Sigui p un nombre primer fixat, definim l'anell $\mathbb{Z}_p$ com el conjunt dels enters p-àdics, on un enter p-àdic és una sèrie formal $\sum_{i\geq 0} a_i p^i$, on $0 \leq a_i \leq p-1$.*

Observació 1.1.2. *De fet, la darrera condició és necessària només per a definir els p-àdics de forma efectiva, ja que degut a la divisió entera qualsevol sèrie formal $x \in \mathbb{Z}[p]$ admet una expressió equivalent a la descrita en la definició.*

Exemple 1.1.3. *Sigui $x \in \mathbb{Z}[3]$ la següent sèrie*

$$x = 5 + 6 \cdot 3 + 2 \cdot 3^2 + 8 \cdot 3^3 + 3^4 + 3^5 + \cdots + 3^n + \cdots$$

Aleshores, com que $5 = 1 \cdot 3 + 2, \quad 6 = 2 \cdot 3, \quad 8 = 3 \cdot 2 + 2,$

$$\begin{aligned} x =& (3+2) \cdot 3^0 + (2 \cdot 3) \cdot 3 + 2 \cdot 3^2 + (2 \cdot 3 + 2) \cdot 3^3 + 3^4 + 3^5 + \cdots \\ =& 2 \cdot 3^0 + 1 \cdot 3 + (2+2) \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 3^4 + 3^5 + \cdots \\ =& 2 + 3 + 3^2 + 3^4 + 2 \cdot 3^5 + 3^6 + \cdots, \end{aligned}$$

d'on se segueix que $x \in \mathbb{Z}_p$.

Observació 1.1.4. *Podem identificar qualsevol enter p-àdic $x = \sum_{i\geq 0} x_i p^i$ amb la seqüència $(x_i)_{i\geq 0}$ on $0 \leq x_i \leq p-1$ per a tot i, de manera que podem identificar els enters p-àdics com el producte cartesià*

$$\prod_{i\geq 0} \{0, 1, \cdots, p-1\} = \{0, \cdots, p-1\}^{\mathbb{N}}.$$

En particular, si $x, y \in \mathbb{Z}_p, x = \sum_{i\geq 0} x_i p^i \;\; y = \sum_{i\geq 0} y_i p^i$ tenim que $x = y \iff x_i = y_i \;\forall i \geq 0$.

Proposició 1.1.5. *El conjunt dels enters p-àdics és, efectivament, un anell amb les operacions següents:*

$x, y \in \mathbb{Z}_p, x = \sum_{i\geq 0} x_i p^i,\ y = \sum_{i\geq 0} y_i p^i.$

- $x + y = \sum_{i\geq 0}(x_i + y_i)p^i = \sum_{i\geq 0} z_i p^i$ *amb* $c_i \equiv x_i + y_i \pmod{p^i}$.

- $x \cdot y = \left(\sum_{i\geq 0} x_i p^i\right) \cdot \left(\sum_{i\geq 0} y_i p^i\right) = \sum_{i\geq 0}\left(\sum_{n=0}^{i} x_n y_{i-n}\right) p^i = \sum_{i\geq 0} z_i p^i$ *amb* $z_n \equiv \sum_{n=0}^{i} x_n y_{i-n} \pmod{p^n}$.

i amb

$$1 = 1 + 0p + 0p^2 + 0p^3 + \cdots,$$
$$0 = 0 + 0p + 0p^2 + 0p^3 + \cdots.$$

Demostració. Això és clar. □

Definició 1.1.6. *Sigui $x = \sum_{i\geq 0} x_i p^i$ un enter p-àdic qualsevol, definim l'ordre de x com el màxim natural n tal que p^n divideix x, és a dir, el mínim natural n tal que $x_n \neq 0$. Podem pensar-ho com una aplicació de la següent manera,*

$$\begin{array}{rccc} \mathrm{ord}_p: & \mathbb{Z}_p \setminus \{0\} & \longrightarrow & \mathbb{N} \\ & x = \sum_{i\geq 0} x_i p^i & \longmapsto & \min\{i;\ x_i \neq 0\}. \end{array}$$

Donat que $x \neq 0$, i que dos enters p-àdics són iguals si coincideixen en totes les seves components, tenim que l'ordre està ben definit.

Podem estendre l'ordre a $\mathbb{Z}_p$ de la manera següent

$$\begin{array}{rccc} \mathrm{ord}_p: & \mathbb{Z}_p & \longrightarrow & \mathbb{N} \cup \{\infty\} \\ & x = \sum_{i\geq 0} x_i p^i & \longmapsto & \begin{cases} \min\{i;\ x_i \neq 0\} & si\ \ x \neq 0, \\ \infty & si\ \ x = 0. \end{cases} \end{array}$$

Lema 1.1.7. *$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ com a anells.*

Demostració. Considerem el morfisme

$$\begin{array}{rccccc} \pi: & \mathbb{Z}_p & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & x = \sum_{i\geq 0} x_i p^i & \longmapsto & x_0 & \longmapsto & \overline{x_0}. \end{array}$$

És clarament un morfisme d'anells. Com que $0 \leq x_0 < p$ tenim que $\pi(x) = 0 \iff x_0 = 0$, per tant, $\ker(\pi) = \{x = \sum_{i\geq 0} x_i p^i;\ \ x_0 = 0\}$.

Ara, si $x \in \ker(\pi)$ tenim $x = x_1 p + x_2 p^2 + \cdots = p(x_1 + x_2 p + x_3 p^2 + \cdots)$, d'on clarament obtenim que $\ker(\pi) = p\mathbb{Z}_p$. A més a més, el morfisme és clarament exhaustiu, per tant, pel primer teorema d'isomorfia s'obté el resultat. □

Proposició 1.1.8. $\mathbb{Z}_p^\star = \{x = \sum_{i\geq 0} x_i p^i; \quad x_0 \neq 0\}$.

Demostració. La inclusió d'esquerra a dreta és trivial. Si un element és invertible, també ho ha de ser $\pi(x)$, per tant, $x_0 \neq 0$. Considerem $x = \sum_{i\geq 0} x_i p^i$ amb $x_0 \neq 0$, aleshores $\pi(x) = \overline{x_0} \neq 0$ per tant, existeix $a \in \mathbb{Z}$ tal que $x_0 a \equiv 1 \pmod p$ és a dir $x_0 a = 1 + rp$, amb $r \in \mathbb{Z}$, de manera que $ax = 1 + y_1 p + y_2 p^2 + \cdots$, per tant, tenim que $ax = 1 + zp$, on $z \in \mathbb{Z}_p$, ara bé, $(1+zp)^{-1} = 1 - zp + (zp)^2 - (zp)^3 + \cdots = 1 + b_1 p + b_2 p^2 + \cdots \in \mathbb{Z}_p$. D'on se segueix que, $a(1+zp)^{-1}x = 1 \implies x^{-1} = a(1+zp)^{-1} \in \mathbb{Z}_p$ □

Proposició 1.1.9. *L'anell $\mathbb{Z}_p$ és domini íntegre.*

Demostració. Vegem que no hi ha divisors de zero. Siguin $x, y \in \mathbb{Z}_p$, aleshores, existeixen sengles enters naturals n, m i sengles unitats ε, η tals que $x = p^n\varepsilon,\ y = p^m\eta$ (això és conseqüència de la proposició precedent). Suposem que $x \cdot y = 0$ aleshores, $p^{n+m}\varepsilon\eta = 0$ multiplicant pels inversos de les unitats obtenim $p^{n+m} = 0$, però això no pot ser.

□

Aquest resultat ens duu a la següent caracterització. Si $x \in \mathbb{Z}_p$ i $n = \mathrm{ord}_p(x)$, tenim que $x = \sum_{i\geq 0} x_i p^i = \sum_{i\geq n} x_i p^i = p^n \sum_{j\geq 0} x_{j+n} p^j$ i $\sum_{j\geq 0} x_{j+n} p^j$ és unitat.

Vegem que aquesta descomposició és única. Suposem que $x = p^n u = p^m v$, on $u, v \in \mathbb{Z}_p$, aleshores, per definició d'ordre $n = m$, i vist que $\mathbb{Z}_p$ és domini íntegre, tenim que $u = v$.

És a dir, hem provat el següent resultat.

Proposició 1.1.10. *Si $x \in \mathbb{Z}_p$ aleshores, existeixen una única unitat u de $\mathbb{Z}_p$ i un únic enter natural n, tals que $x = p^n \cdot u$*

□

Aquesta és la condició usual d'uniformitzant. Recordem algunes conseqüències de l'existència d'uniformitzant.

Lema 1.1.11. *Sigui A és un anell commutatiu, unitari i íntegre. Si A admet un uniformitzant τ els seus ideals són de la forma (τ^r) amb $r \in \mathbb{N}$.*

Demostració. cf. [2]. □

Corol·lari 1.1.12. *L'anell $\mathbb{Z}_p$ és un domini d'ideals principals i anell Noetherià.*

Demostració. La primera condició és clara dels dos resultats precedents. La Noetherianitat és dedueix del fet que si $\{I_j\}_{j\in J}$ és una cadena d'ideals, per a tot $j \in J$ existeix $n_j \in \mathbb{N}$ tal que $I_j = (p^{n_j})$, de manera que està inclosa en la cadena següent:

$$(p) \supseteq (p^2) \supseteq (p^3) \supseteq \cdots \supseteq (p^m) \supseteq \cdots.$$

Aquesta cadena estaciona, d'on obtenim que la cadena $\{I_j\}_{j\in J}$ estaciona. □

També ens dóna una manera diferent de mirar-nos la valoració que hem definit.

Proposició 1.1.13. *Sigui A un anell commutatiu unitari i íntegre, no cos. Són equivalents*

(i) A admet un uniformitzant.

(ii) A és un anell de valoració discreta.

Demostració. cf. [2] □

La condició de no cos ja l'hem vista implícitament quan hem vist que les unitats són exactament les que tenen ordre igual a 0. De fet, la manera de demostrar que (i) implica (ii) és definint la valoració v com a $v(x) = n \iff x = \tau^n u$ amb τ uniformitzant i u unitat. Per tant, obtenim que la valoració p-àdica ord_p és una valoració discreta. És a dir, satisfà les condicions

$$\begin{cases} \mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \\ \mathrm{ord}_p(a+b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \end{cases}$$

sempre que $a, b, a+b \neq 0$.

Definició 1.1.14. *Denotarem al cos de fraccions de $\mathbb{Z}_p$ com $\mathbb{Q}_p$.*

Lema 1.1.15. $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

Demostració. Com que les valoracions discretes venen definides d'un cos k en $\mathbb{Z}$, i com que $\mathbb{Z}_p$ és l'anell de valoració de ord_p obtenim que podem prendre $k = \mathbb{Q}_p$.

Si $x \in \mathbb{Q}_p$ i $\mathrm{ord}_p(x) = r < 0$ aleshores, $\mathrm{ord}_p(xp^{-r}) = \mathrm{ord}_p(x) + \mathrm{ord}_p(p^{-r}) = r - r = 0$, així, $xp^{-r} \in \mathbb{Z}_p$, ara $xp^{-r} = \sum_{i\geq 0} y_i p^i$, per tant,

$$x = \sum_{i\geq 0} y_i p^{i+r},$$

i com que r és negatiu, la sèrie és una sèrie de Laurent. D'on se segueix el resultat. □

1.2 Límits projectius.

Definició 1.2.1. *Per a cada $n \geq 1$, definim un parell (E_n, φ_n) on E_n és un conjunt i $\varphi_n : E_{n+1} \longrightarrow E_n$ és una aplicació per a cada natural n. Anomenem a la seqüència $(E_n, \varphi_n)_{n\geq 1}$ sistema projectiu.*

Si $(E_n, \varphi_n)_{n\geq 1}$ és un sistema projectiu i E és un conjunt tal que per a cada natural $n \geq 1$ existeix un morfisme

$$\psi_n : E \longrightarrow E_n$$

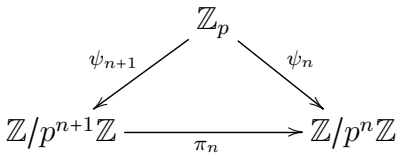
de manera que $\psi_n = \varphi_n \circ \psi_{n+1}$ es diu que E és el límit projectiu del sistema $(E_n, \varphi_n)_n$. Ho escrivim

$$E = \varprojlim(E_n, \varphi_n).$$

Proposició 1.2.2. *Sigui $\mathbb{Z}/p^n\mathbb{Z}$ i $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ la projecció natural. Aleshores,*

$$\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}, \pi_n).$$

Demostració. Només hem de veure que per a cada $n \geq 1$ existeixen ψ_n, ψ_{n+1} tals que el diagrama



commuta.

Sigui $x \in \mathbb{Z}_p$, aleshores $x = \sum_{i\geq 0} x_i p^i$, definim

$$\psi_n(x) = \sum_{i=0}^{n-1} x_i p^i.$$

Aquesta aplicació fa commutar el diagrama, ja que $\pi_n(\psi_{n+1}(x)) = \pi_n(\sum_{i=0}^{n} x_i p^i) \equiv \sum_{i=0}^{n-1} x_i p^i \pmod{p} = \psi_n(x)$. □

Com que hem vist que $\mathbb{Z}_p$ és un límit projectiu, és a dir, el conjunt de les seqüències $(x_n)_n$ on $x_n \equiv x_m \pmod{p^n}$ si $m \geq n$ per a qualsevol n, podem pensar-lo com a subconjunt del producte $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$. Si dotem a $\mathbb{Z}/p^n\mathbb{Z}$ amb la topologia discreta i a $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ de la topologia producte, obtenim una topologia a $\mathbb{Z}_p$ com a subconjunt, de manera que el fa un conjunt compacte ja que és tancat en un producte d'espais compactes.

Proposició 1.2.3. *La topologia que hem definit es pot obtenir també mitjançant la distància*

$$d(x, y) = p^{-\mathrm{ord}_p(x-y)}.$$

A més a més, $\mathbb{Z}_p$ és un espai mètric complet i $\mathbb{Z}$ hi és dens.

Anàlogament, $\mathbb{Q}_p$ amb la topologia definida per la distància anterior, és localment compacte i conté $\mathbb{Z}_p$ com a subanell obert. $\mathbb{Q}$ hi és dens.

Demostració. Cf. [3],[12]. □

Definició 1.2.4. *Definim per a tot* $x \in \mathbb{Z}_p$

$$|x|_p = p^{-\mathrm{ord}_p(x)}$$

la norma p-àdica. Es pot comprovar fàcilment que és norma i que $d(x,y) = |x-y|_p$ *trivialment.*

Observació 1.2.5. *Si* $x, y \in \mathbb{Z}_p$ *tenim en general que*

$$|x+y|_p \leq \max(|x|_p, |y|_p)$$

però es pot demostrar fàcilment que si $|x|_p \neq |y|_p$ *es dóna la igualtat.*

Demostració. Cf [3]. □

1.3 Equacions p-àdiques

L'objectiu principal d'aquesta secció és estudiar les propietats fonamentals de les equacions dins dels anells i cossos p-àdics, per arribar més tard al cas específic en què els coeficients són enters, aquesta reducció té sentit donat que els enters p-àdics estenen els enters i anàlogament amb els racionals; aquesta reducció ens portarà finalment al comportament local-global dels zeros d'uns certs polinomis sota unes condicions que veurem més endavant.

Lema 1.3.1. *Sigui* $\{D_n, \varphi_n\}_{n\in\mathbb{N}}$ *un sistema projectiu, sigui* $D = \varprojlim D_n$ *el seu límit projectiu. Si per a cada n tenim que* D_n *és finit, aleshores D és no buit si, i només si, per a cada n* D_n *és no buit.*

Demostració. Hem de veure que ens podem reduir al cas en què φ_n és exhaustiu per a qualsevol n, ja que en aquest cas podem construir un element del límit projectiu de la següent manera. Sigui $x_1 \in D_1$ que existeix perquè és no buit, ara, com que φ_1 és exhaustiva, existeix $x_2 \in \varphi_1^{-1}(x_1)$, seguint aquest raonament, sabem que existeix un nombre finit d'elements en $\varphi_n^{-1}(x_n)$ i per exhaustivitat són conjunts amb almenys un element. D'on obtenim que el límit projectiu no pot ser buit.

Ara, fixat $n \in \mathbb{N}$, per a qualsevol m podem definir $D_{n,m} = \varphi_{n+m-1} \circ \cdots \circ \varphi_n$, és a dir, considerem la imatge de D_{n+m} dins de D_n mitjançant la composició dels morfismes

$$D_{n+m} \xrightarrow{\varphi_{n+m-1}} D_{n+m-1} \xrightarrow{\varphi_{n+m-2}} D_{n+m-2} \xrightarrow{\varphi_{n+m-3}} \cdots \xrightarrow{\varphi_n} D_n.$$

Donat que $\varphi_{n+m-1}(D_{n+m}) \subseteq D_{n+m-1}$ tenim una cadena decreixent de conjunts finits de la manera següent:

$$D_{n,m} \subseteq D_{n,m-1} \subseteq D_{n,m-2} \subseteq \cdots \subseteq D_n.$$

Per tant, la cadena és estacionària, que és el mateix que dir que per a m, n prou grans les cadenes construïdes amb aquests naturals coincidiran, és a dir, la cadena és independent de l'elecció de l'enter si aquest és prou gran. Considerem doncs E_n com el límit d'aquesta cadena estacionària. De $D_n \to D_{n-1}$ obtenim clarament que podem posar $E_n \to E_{n-1}$ amb l'aplicació induïda. Aquests conjunts són no buits i finits, a més a més, les aplicacions induïdes són exhaustives per construcció, i pel que hem vist això ens implica que $\varprojlim E_n$ és no buit, per tant, D tampoc ho pot ser.

El recíproc és clar, si tenim elements en D aquests indueixen elements en D_n per a qualsevol n. □

Definició 1.3.2. *Sigui $x = (x_1, \cdots, x_m) \in (\mathbb{Z}_p)^m$, diem que x és un punt primitiu (o bé, una solució o zero primitiu si ens referim a un zero o solució d'un polinomi o equació) si existeix $1 \leq i \leq m$ un nombre natural tal que x_i és no divisible per p, i.e., x_i és invertible. Anàlogament, per a $(\mathbb{Z}/p^n\mathbb{Z})^m$.*

El lema anterior ens permet demostrar la proposició següent.

Proposició 1.3.3. *Siguin $f_i \in \mathbb{Z}_p[X_1, \cdots, X_m]$ una família arbitrària de polinomis amb coeficients en l'anell dels enters p-àdics. Aleshores, són equivalents*

(i) Els f_i tenen un zero primitiu en comú en $(\mathbb{Z}_p)^m$.

(ii) Els f_i tenen un zero no trivial en comú en $(\mathbb{Q}_p)^m$.

(iii) Si considerem $f_i^{(n)}$ la projecció dels polinomis f_i en $\mathbb{Z}/p^n\mathbb{Z}$, aleshores tenen un zero primitiu en comú a $(\mathbb{Z}/p^n\mathbb{Z})^m$ per a tot natural $n \geq 1$.

Demostració. Veure que (i) implica (ii) és trivial. Recíprocament, sigui $x = (x_1, \cdots, x_m)$ un zero no trivial dels f_i, considerem

$$h = \inf \{\mathrm{ord}_p(x_1), \cdots, \mathrm{ord}_p(x_n)\}$$

i definim $y = p^{-h}x$. Clarament y és un punt primitiu de $(\mathbb{Z}_p)^m$, també és clar que és un zero de f_i per a tot i.
Vegem que (i) és equivalent a (iii). Considerem

$$D = \{x \in (\mathbb{Z}_p)^m : \ f_i(x) = 0 \quad \forall i\}.$$

$$D_n = \left\{x \in (\mathbb{Z}/p^n\mathbb{Z})^m : \ f_i^{(n)}(x) = 0 \quad \forall i\right\}.$$

Aleshores, tenim que D_n és finit per a tot n i que $D = \varprojlim D_n$, i pel lema anterior, D és no buit si, i només si, D_n és no buit per a tot n. □

En molts casos el càlcul de solucions p-àdiques pot ser difícil donat que es tracten de sèries formals infinites. Emperò, no sempre és necessari calcular-les per poder assegurar-ne l'existència. Vegem algun lema en aquesta direcció.

Lema 1.3.4. *Sigui $f \in \mathbb{Z}_p[X]$ és un polinomi amb coeficients en $\mathbb{Z}_p$, denotarem f' a la seva derivada formal. Sigui $x \in \mathbb{Z}_p$ i $n, k \in \mathbb{Z}$ tals que $0 \leq 2k \leq n$, $f(x) \equiv 0 \pmod{p^n}$ i $\operatorname{ord}_p(f'(x)) = k$. Aleshores, podem assegurar l'existència d'un $y \in \mathbb{Z}_p$ tal que*

$$f(y) \equiv 0 \pmod{p^{n+1}}, \quad \operatorname{ord}_p(f'(x)) = k, \quad y \equiv x \pmod{p^{n-k}}.$$

Demostració. De les hipòtesis tenim que $f(x) = p^n b$ on $b \in \mathbb{Z}_p$ i $f'(x) = p^k c$ on $c \in \mathbb{Z}_p^*$. Sigui $z \in \mathbb{Z}_p$ tal que $b + zc \equiv 0 \pmod{p}$, aleshores, escollim $y = x + p^{n-k}z$. Del desenvolupament de Taylor de f

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} a,$$

on $a \in \mathbb{Z}_p$ obtenim que

$$f(y) = p^n(b + zc) + p^{2n-2k} a \equiv 0 \pmod{p^{n+1}},$$

ja que $2n - 2k > k$. Clarament $y \equiv x \pmod{p^{n-k}}$. Aplicant la fórmula de Taylor a $f'(y)$ obtenim que $f'(y) \equiv p^k c \pmod{p^{n-k}}$ i donat que $n-k > k$ tenim que $\operatorname{ord}_p(f'(y)) = k$. □

De fet, el que ens interessa provar és una versió més general del Lema de Hensel que ens servirà en capítols posteriors.

Lema 1.3.5 (Lema de Hensel general)**.** *Sigui $f \in \mathbb{Z}_p[X]$, denotarem per f' a la seva derivada formal. Sigui $a \in \mathbb{Z}_p$ tal que $|f(a)|_p < |f'(a)|_p^2$. Aleshores existeix un únic enter p-àdic α tal que $f(\alpha) = 0$ i $|\alpha - a|_p < |f'(a)|_p$. A més a més,*

(a) $|\alpha - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p < |f'(a)|_p$.

(b) $|f'(\alpha)|_p = |f'(a)|_p$.

Demostració. En primer lloc definirem una successió $\{a_n\}_n \subseteq \mathbb{Q}_p$ de la manera següent, $a_1 = a$ i si $n > 1$ aleshores, $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. Posem $c = \left|\frac{f(a)}{f'(a)^2}\right|_p < 1$. Provarem per inducció els següents tres punts

(i) $|a_n|_p \leq 1$ per a tot $n \geq 1$, donat que $\mathbb{Z}_p$ és l'anell de valoració de $\mathbb{Q}_p$ aquesta condició és equivalent a què $\operatorname{ord}_p(a_n) \geq 0$ per a tot $n \geq 1$, és a dir $a_n \in \mathbb{Z}_p$.

(ii) $|f'(a_n)|_p = |f'(a_1)|_p$ per a tot $n \geq 1$.

(iii) $|f(a_n)|_p \leq |f'(a_1)|_p^2 c^{2^{n-1}}$.

Per a $n = 1$ els tres punts són clars. Vegem el pas inductiu: suposem cert per a $n > 1$.

Per a veure-ho necessitem dues identitats polinomials.

(I1) Si $F \in \mathbb{Z}_p[X]$, $F(X+Y) = F(X) + F'(X)Y + G(X,Y)Y^2$ per a algun polinomi $G(X,Y) \in \mathbb{Z}_p[X,Y]$.

(I2) Si $H(X) \in \mathbb{Z}_p[X]$ tenim $H(X) - H(Y) = (X-Y)P(X,Y)$, per a algun polinomi $P(X,Y) \in \mathbb{Z}_p[X,Y]$.

Per a deduir (I1) escrivim $F(X) = \sum_{i=0}^{d} c_i X^i$, aleshores

$$F(X+Y) = \sum_{i=0}^{d} c_i (X+Y)^i = c_0 + \sum_{i=1}^{d} c_i (X^i + iX^{i-1}Y + G_i(X,Y)Y^2)$$
$$= \sum_{i=0}^{d} c_i X^i + \sum_{i=1}^{d} c_i i X^{i-1} Y + Y^2 \sum_{i=1}^{d} G_i(X,Y) = F(X) + F'(X)Y + G(X,Y)Y^2.$$

La identitat (I2) la deduïm del següent raonament. Sigui $H(X) = \sum_{i=0}^{r} b_i X^i$, aleshores,

$$H(X) - H(Y) = \sum_{i=1}^{r} b_i (X^i - Y^i).$$

Observem que el terme independent desapareix i que per a tot $i \geq 1$ tenim que $X - Y$ divideix $X^i - Y^i$, d'on obtenim que

$$H(X) - H(Y) = (X-Y)P(X,Y)$$

per a algun polinomi $P(X,Y) \in \mathbb{Z}_p[X,Y]$

Observem que I1 ens permet afirmar fent $F(X) = f(X)$ que per a $x, y \in \mathbb{Z}_p$

$$f(x+y) = f(x) + f'(x)y + zy^2$$

per a algun $z \in \mathbb{Z}_p$. De la segona identitat tenim que $H(x) - H(y) = (x-y)z$ amb $z \in \mathbb{Z}_p$, per tant, $|z|_p \leq 1$, perquè $\mathbb{Z}_p$ és l'anell de valoració de $\mathbb{Q}_p$. D'on se segueix que

$$|H(x) - H(y)|_p \leq |x-y|_p$$

per a tot polinomi $H(X) \in \mathbb{Z}_p[X]$

Provem doncs el punt (i): en primer lloc observem que a_{n+1} està definit, ja que per hipòtesi d'inducció $|f'(a_n)|_p = |f'(a)|_p > |f(a)| \geq 0$. A més a més, podem suposar que $f(a) \neq 0$, altrament ja estaríem. $|a_{n+1}|_p \leq 1$ és equivalent a $a_{n+1} \in \mathbb{Z}_p$ i donat que per hipòtesi $a_n \in \mathbb{Z}_p$ hem de veure que $\frac{f(a_n)}{f'(a_n)} \in \mathbb{Z}_p$. És a dir, que la seva norma és menor o igual que 1. Fent servir (ii) i (iii) per a n tenim que

$$\left|\frac{f(a_n)}{f'(a_n)}\right|_p = \left|\frac{f(a_n)}{f'(a_1)}\right|_p \leq |f'(a_1)|_p c^{2^{n-1}} \leq 1,$$

ja que $c < 1$.

Per a provar (ii) fem servir la identitat (I2) amb $H(X) = f'(x)$

$$|f(a_{n+1}) - f(a_n)|_p \leq |a_{n+1} - a_n|_p = \left|\frac{f(a_n)}{f'(a_n)}\right|_p = \left|\frac{f(a_n)}{f'(a_1)}\right|_p < |f'(a_1)|_p.$$

On la última desigualtat es dedueix fent servir (iii). Ara, suposem que $|f'(a_{n+1})|_p \neq |f'(a_n)|_p$ aleshores, per la observació 1.2.5 tenim que

$$|f'(a_{n+1}) - f'(a_n)|_p = \max(|f'(a_{n+1})|_p, |f'(a_n)|_p) = \max(|f'(a_{n+1})|_p, |f'(a_1)|_p)$$

Si el màxim és $|f'(a_n)|_p = |f'(a_1)|_p$ obtenim $|f'(a_1)|_p < |f'(a_1)|_p$ que és una contradicció. Si el màxim és $|f'(a_{n+1})|_p$, aleshores obtenim que $|f'(a_{n+1})|_p > |f'(a_1)|_p$ i pel que hem deduït de la identitat (I2) tenim $|f'(a_{n+1})|_p < |f'(a_1)|_p$ que de nou és una contradicció. Per tant, $|f'(a_{n+1})|_p = |f'(a_n)|_p = |f'(a_1)|_p$. Com volíem veure.

Vegem finalment el punt (iii). Fem servir la identitat (I1) amb $F(X) = f(X)$, $x = a_n$ i $y = -\frac{f(a_n)}{f'(a_n)}$, d'on se segueix que

$$f(a_{n+1}) = f\left(a_n - \frac{f(a_n)}{f'(a_n)}\right) = f(a_n) - f'(a_n)\frac{f(a_n)}{f'(a_n)} + z\left(\frac{f(a_n)}{f'(a_n)}\right)^2 = z\left(\frac{f(a_n)}{f'(a_n)}\right)^2,$$

per a algun $z \in \mathbb{Z}_p$. Per tant, fent servir la hipòtesi d'inducció i que $z \in \mathbb{Z}_p \implies |z|_p \leq 1$.

$$|f(a_{n+1})|_p \leq \left|\frac{f(a_n)}{f'(a_n)}\right|_p^2 \leq \left(|f'(a_1)|_p^2 c^{2^{n-1}}\right)^2 \frac{1}{|f'(a_1)|_p^2} = |f'(a_1)|_p^2 c^{2^n}.$$

Per tant, queden provats els tres punts. Vegem ara que la successió $\{a_n\}_n$ és una successió de Cauchy.

$$|a_{n+1} - a_n|_p = \left|\frac{f(a_n)}{f'(a_n)}\right| = \frac{|f(a_n)|_p}{|f'(a_1)|_p} \leq |f'(a_1)|c^{2^{n-1}}.$$

I com que $0 < c < 1$, la successió és de Cauchy. Sabem que $\mathbb{Q}_p$ és un espai mètric complet (1.2.3). Sigui doncs $\alpha = \lim_n a_n$, passant al límit $|a_n|_p \leq 1$ tenim que $|\alpha|_p \leq 1$, d'on obtenim $\alpha \in \mathbb{Z}_p$. De nou, passant al límit $|f'(a_n)|_p = |f'(a_1)|_p$ obtenim $|f'(\alpha)|_p = |f'(a_1)|_p$ i de $|f(a_n)| \leq |f'(a_1)|_p^2 c^{2^{n-1}}$ obtenim que $|f(\alpha)| = 0$ que implica $f(\alpha) = 0$.

Només ens queda veure que $|\alpha - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p$, provarem $|a_n - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p$ per a tot $n \geq 2$ i després passarem al límit. Fem-ho per inducció, per a $n = 2$ és clar de la definició de a_2 en termes de a. Per a tot $n \geq 2$ tenim

$$|a_{n+1}-a_n|_p \leq |f'(a)|_p c^{2^{n-1}} \leq |f(a)|_p c^2 < |f'(a)|c = \left|\frac{f(a)}{f'(a)}\right|_p .$$

Per hipòtesi d'inducció $|a_n - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p$ per tant tenim que $|a_{n+1}-a_n| < |a_n-a|_p$ per tant, $|a_{n+1}-a|_p = |(a_{n+1}-a_n)+(a_n-a)|_p = |a_n-a|_p = \left|\frac{f(a)}{f'(a)}\right|_p$.

Finalment, vegem que α és la única arrel de $f(X)$ en la bola $\{x \in \mathbb{Z}_p : \ |x-a|_p < |f'(a)|_p\}$. Suposem que existeix un element β amb les mateixes característiques que α, és a dir, $f(\beta) = 0$ i $|\beta - a|_p < |f'(a)|_p$. Com que $|\alpha - a|_p < |f'(a)|_p$ tenim que $|\beta-\alpha|_p < |f'(a)|_p$, escrivim $\beta = \alpha + h$ on $h \in \mathbb{Z}_p$, i per la identitat (I1) tenim

$$0 = f(\beta) = f(\alpha) + f'(\alpha)h + zh^2 = f'(\alpha)h + zh^2,$$

per a algun $z \in \mathbb{Z}_p$. Suposem que $h \neq 0$, aleshores $f'(\alpha) = -hz$ i $|f'(\alpha)|_p \leq |h|_p = |\beta-\alpha|_p < |f'(a)|_p$ però per hem demostrat que $|f'(\alpha)|_p = |f'(a)|_p$, i això genera una contradicció. Així, $h = 0$ i $\beta = \alpha$. □

Corol·lari 1.3.6 (Lema de Hensel)**.** *Sigui $f \in \mathbb{Z}_p[X]$ (o bé amb coeficients enters) un polinomi, sigui f' la seva derivada. Si existeix un enter $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod p$ i que $f'(a) \not\equiv 0 \pmod p$ aleshores, existeix una única solució b p-àdica de f tal que $b \equiv a \pmod p$.*

Demostració. Això és conseqüència del lema de Hensel general. De la hipòtesi $f'(a) \not\equiv 0 \pmod 3$ tenim que $\mathrm{ord}_p f'(a) = 0$ i per tant $|f'(a)|_p = 1$. Així, com que $f(a) \equiv 0 \pmod p$ tenim que $|f(a)|_p < 1 = |f'(a)|_p^2$ i en conseqüència aplica el lema de Hensel general. □

Observació 1.3.7. *Fem abús de notació amb els polinomis de $\mathbb{Z}/p^n\mathbb{Z}$ i $\mathbb{Z}_p$, però això no és causa d'error en els resultats. Quan ens referim a un polinomi amb coeficients p-àdics i després el considerem en $\mathbb{Z}/p^n\mathbb{Z}$ ho fem mitjançant el morfisme ψ_n que hem demostrat que existeix en la secció anterior.*

Lema 1.3.8. *Siguin $m, n, k, j \in \mathbb{Z}$ tals que $0 \leq j \leq m$. Sigui $f \in \mathbb{Z}_p[X_1, \cdots, X_m]$, $x = (x_1, \cdots, x_m) \in (\mathbb{Z}_p)^m$. Suposem $0 < 2k < n$ i què*

$$f(x) \equiv 0 \pmod{p^n} \text{ i } \mathrm{ord}_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Aleshores, existeix un zero de f en $(\mathbb{Z}_p)^m$ que és congruent a x mòdul $pn-k$.

Demostració. Fem-ho per inducció sobre m. El cas $m = 1$ fem servir el Lema de Hensel. Si $m > 1$, considerem el polinomi $\overline{f} \in \mathbb{Z}_p[X_j]$ que s'obté de substituir en f X_i per x_i sempre que $i \neq j$. Això és el cas $m = 1$ que ja hem vist. Fem això per a tot j i resulta el què buscàvem. □

1.4 Cossos finits

En la secció anterior hem vist com podem assegurar l'existència de solucions p-àdiques si sabem l'existència d'una solució en un cos finit. Però per obtenir resultats més generals, necessitem poder assegurar l'existència de solucions en aquests cossos finits.

El resultat més important és el següent.

Teorema 1.4.1 (Chevalley-Warning)**.** *Considerem un cos finit $\mathbb{F}_q$ de característica p primer amb q elements. Siguin $(f_i)_i \subset \mathbb{F}_q[X_1, \cdots, X_n]$ una família de polinomis amb la condició que*

$$\sum_i \deg f_i < n,$$

i sigui

$$V = \left\{x \in \mathbb{F}_q^n;\ f_i(x) = 0\ \forall i\right\}.$$

Aleshores,

$$|V| \equiv 0 \pmod{p}.$$

Demostració. Considerem el següent polinomi

$$P = \prod_i (1 - f_i^{q-1}).$$

Si $x \in V \implies f_i(x) = 0$ per a tot i per tant, $P(x) = 1$. Si $x \notin V \implies f_i(x)^{q-1} = 1$ per almenys un f_i i ja que estem en un cos finit. Aleshores, $P(x) = 0$. D'on se segueix que P és la funció característica del conjunt V. Per tant,

$$|V| = \sum_{x \in \mathbb{F}_q^n} P(x).$$

Si vegem $\sum_{x \in \mathbb{F}_q^n} P(x) = 0$ ja estarem. De fet, es tracta d'una congruència donat que els elements x els operem a $\mathbb{F}_q$.

Primerament,

$$\deg(P) = \sum_i \deg\left(1 - f_i^{q-1}\right) \leq \sum_i (q-1)\deg(1 - f_i) \leq (q-1)\sum_i \deg(f_i) < (q-1)n.$$

Ara, sabem que P és combinació lineal de termes $X^r = X_1^{r_1} \cdots X_n^{r_n}$ i que $\sum r_i < n(q-1)$. Provarem que $\sum_{x \in \mathbb{F}_q^n} x^r = 0$ per a tot monomi X^r que aparegui en P. Donat que almenys un r_i és més petit que $q-1$ tenim que no és divisible per $q-1$ i per tant, existeix un element $y \in \mathbb{F}_q$ tal que $y^r \neq 1$ i en conseqüència

$$\sum_{x \in \mathbb{F}_q^*} x^r = \sum_{x \in \mathbb{F}_q^*} y^r x^r = y^r \sum_{x \in \mathbb{F}_q^*} x^r.$$

Com que $y^r \neq 1$ tenim $\sum_{x \in \mathbb{F}_q^*} x^r = 0$, com volíem veure. □

Corol·lari 1.4.2. *Amb les mateixes condicions, si $\sum_i \deg(f_i) < n$ i els f_i no tenen terme constant, aleshores tenen un zero en comú no trivial.*

Demostració. Això és clar, si $V = \{0\} \implies |V| \equiv 1 \pmod{p}$ que contradiu el teorema. Per tant, V té algun element diferent del zero. □

Corol·lari 1.4.3. *Amb les mateixes condicions, si f és un polinomi homogeni de grau 2 (és a dir, una forma quadràtica) en almenys 3 variables sobre $\mathbb{F}_q$, té un zero no trivial.*

1.5 Unitats i quadrats p-àdics

Per a poder donar una descripció efectiva de l'estructura dels anells i cossos p-àdics necessitem estudiar l'estructura que formen les unitats i els quadrats.

En primer lloc, per a poder estructurar les unitats del cos $\mathbb{Q}_p$, definim els morfismes següents.

$$\begin{array}{rccc} \varphi_n : & \mathbb{Z}_p^* & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})^* \\ & \sum_{n\geq 0} x_n p^n & \longmapsto & x_0 + x_1 p + \cdots + x_{n-1}p^{n-1}. \end{array}$$

Ara considerem els nuclis d'aquests morfismes. Sigui $x \in \mathbb{Z}_p$ tal que per a un n tenim que $\varphi_n(x) = 0$, aleshores tenim que $x_0 = 1$ i $x_i = 0$ per a tot $i \leq n-1$. Anàlogament, si es compleix aquesta propietat per a un element x la seva imatge és la classe del 1. Per tant, $\ker(\varphi_n) = 1 + p^n\mathbb{Z}_p$.

Considerem ara l'aplicació

$$\begin{array}{ccc} 1 + p^n\mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ 1 + xp^n & \longmapsto & x \pmod{p} \end{array}$$

Es tracta d'un morfisme de grups. En efecte, només cal comprovar que

$$(1 + p^n x)(1 + p^n y) \equiv 1 + p^n(x + y) \pmod{p^{n+1}}.$$

El seu nucli són els elements $1 + xp^n$ on p divideix x, per tant,

$$(1 + p^n\mathbb{Z}_p)/(1 + p^{n+1}\mathbb{Z}_p) \simeq \mathbb{F}_p.$$

Podem observar també que, donat que $\mathbb{Z}_p^* \supseteq 1 + p^n\mathbb{Z}_p \supseteq 1 + p^{n+1}\mathbb{Z}_p$ es pot comprovar fàcilment que

$$\mathbb{Z}_p^* = \varprojlim \mathbb{Z}_p^*/(1 + p^n\mathbb{Z}_p).$$

D'aquesta manera podem deduir l'estructura de les unitats.

Lema 1.5.1. *$\mathbb{Z}_p^*$ conté les arrels $p-1$-èssimes de la unitat.*

Demostració. Considerem el polinomi $f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Pel lema de Hensel, sigui x_0 un enter qualsevol $0 < x_0 < p$, aleshores $x_0 \not\equiv 0 \pmod{p}$. I $f(x_0) \equiv 0 \pmod{p}$. La derivada formal de f és $f'(X) = (p-1)X^{p-2}$, i $f'(x_0) \equiv -x_0^{p-2} \not\equiv 0$, ja que x_0 no és divisible per p. Per tant, existeix una solució p-àdica x de $f(X) = 0$, i aquesta solució és una arrel $p-1$-èssima de la unitat. Si $x_0 \neq 1$ aquesta solució és primitiva i tenim totes les arrels de $f(X)$ a $\mathbb{Z}_p^*$. □

Proposició 1.5.2. *L'estructura de les unitats pot ser donada per*

$$\mathbb{Z}_p^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

on $\mu_{p-1} = \left\{x \in \mathbb{Z}_p^*;\ x^{p-1} = 1\right\}$.

Demostració. Sigui $x \in \mathbb{Z}_p^*$, aleshores $(x_0, x_1, x_2, \cdots) \in \mathbb{Z}_p^*$, on ens mirem l'element dins l'estructura de límit projectiu. Pel lema anterior, com que $x_0 \neq 0$ ja que x és unitat, existeix $y \in \mathbb{Z}_p^*$ tal que $y^{p-1} = 1$, tal que si $y = (y_0, y_1, \cdots)$ tenim que $x_0 \equiv y_0 \pmod{p}$, i per tant, l'element $y^{-1}x = (1, z_1, z_2, \cdots)$, per tant, $y^{-1}x \in (1+p\mathbb{Z}_p)$. Ara, si $x \in \mu_{p-1} \cap (1+p\mathbb{Z}_p)$ tenim que $x = (x_0, x_1, \cdots)$, i $x_0 = 1$, però per Hensel, sabem que només existeix una solució tal que $x_0 = 1$ i $x^{p-1} = 1$ i $x = (1, 1, 1, \cdots)$, n'és una. Per tant, $x = 1$. D'on se segueix el resultat. □

Proposició 1.5.3. *Sigui p un nombre primer $p \neq 2$, aleshores*

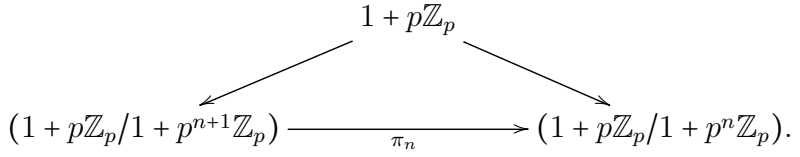
$$1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p.$$

Demostració. Vegem que per a tot n el grup $(1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p)$ és cíclic d'ordre p^{n-1}. Sigui $\alpha = 1 + p$, vegem que si $\overline{\alpha} \in (1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p)$ és la imatge en el quocient, tenim que $\overline{\alpha}^{p^{n-2}} \neq 1$. Si fos així, $\alpha^{p^{n-2}} \in 1 + p^n\mathbb{Z}_p$, però per la fórmula del binomi $(1+p)^p = 1 + p^2 + \cdots + p^p$, per tant això no pot ser. I com que $(1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p)$ és d'ordre p^{n-1} tenim que $\overline{\alpha}^{p^{n-1}} = 1$ i és un generador del grup.

Ara, volem veure que $1 + p\mathbb{Z}_p = \varprojlim(1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p)$, si

$$\pi_n : (1 + p\mathbb{Z}_p/1 + p^{n+1}\mathbb{Z}_p) \longrightarrow (1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p),$$

on $\pi_n(x) = \overline{x}$ és la projecció. Està ben definida perquè els subgrups $1 + p^n\mathbb{Z}_p$ estan encadenats i tenim que el diagrama següent commuta



Ara, vegem que podem establir un isomorfisme entre $\varprojlim \mathbb{Z}/p\mathbb{Z}$ i $\varprojlim(1 + p\mathbb{Z}_p/1 + p^n\mathbb{Z}_p)$.

Només cal veure que podem fer un isomorfisme entre $\mathbb{Z}/p^n\mathbb{Z}$ i $(1+p\mathbb{Z}_p/1+p^{n+1}\mathbb{Z}_p)$ que respecti els morfismes de la condició de límit projectiu, però això és evident fent servir que tenim un generador dels grups que són cíclics i fan commutar el diagrama

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow[\delta_n]{} & (1+p\mathbb{Z}_p/1+p^{n+1}\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^{n-1}\mathbb{Z} & \xrightarrow[\delta_{n-1}]{} & (1+p\mathbb{Z}_p/1+p^{n}\mathbb{Z}_p), \end{array}$$

on $\delta_n(z) = \overline{\alpha}^z$. □

Proposició 1.5.4. *Si $p = 2$, aleshores $1 + 2\mathbb{Z}_2 = \{1, -1\} \times \mathbb{Z}_2$.*

Demostració. La prova és molt semblant a l'anterior, només hem de tenir en compte que l'elecció de α només és possible si comencem en $(1+2^2\mathbb{Z}_2^*)$ i què $(1+2\mathbb{Z}_2)/(1+4\mathbb{Z}_2) \simeq \mathbb{Z}/2\mathbb{Z}$. □

Teorema 1.5.5. *Sigui p un nombre primer, aleshores*

$$\mathbb{Q}_p^* \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p & si\ p \neq 2 \\ \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 & si\ p = 2 \end{cases}.$$

Demostració. Tot element no nul x de $\mathbb{Q}_p$ es pot escriure de manera única com $x = p^n u$, on $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$.

□

Determinem ara l'estructura del grup quocient de les unitats p-àdiques mòdul quadrats.

Teorema 1.5.6. *Si $p \neq 2$ és un nombre primer, aleshores*

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq C_2 \times C_2.$$

Si $p = 2$, tenim

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq C_2 \times C_2 \times C_2,$$

on C_2 denota el grup cíclic d'ordre 2.

Demostració. És immediat de veure que $x \in \mathbb{Q}_p^*$ és quadrat si, i només si, $x = p^n u$ on n és parell i $\overline{x} \in \mathbb{F}_p^*$ la imatge del pas al quocient és un quadrat. En el cas $p = 2$ s'han de considerar més casos donat que $\mathbb{Q}_2$ té una estructura diferent que $\mathbb{Q}_p$ amb $p \neq 2$. Es pot trobar una demostració al llibre de Borevitch-Shafarevitch [3]. □

Capítol 2

El símbol de Hilbert

2.1 Propietats locals

Definició 2.1.1. *Sigui V el conjunt de tots els primers de $\mathbb{Z}$ incloent-hi el primer de l'infinit, ens referirem a $\mathbb{Q}_v$ per a tot $v \in V$ ($\mathbb{Q}_\infty = \mathbb{R}$), posarem k per referir-nos als cossos p-àdics. Siguin $a, b \in k^*$, definirem el símbol de Hilbert de la següent manera*

$$(a,b) = \begin{cases} 1 & \text{si } z^2 - ax^2 - by^2 = 0 \text{ té alguna solució } (x,y,z) \neq (0,0,0) \\ -1 & \text{altrament.} \end{cases}$$

Notem que el símbol de Hilbert depèn del cos k.

De fet, el valor de $(a,b) = (s^2a,b) = (a,r^2b)$, per a $s,r \in k$, motiu pel qual podem reduir el càlcul de (a,b) als factors no quadràtics de a i b.

Vegem algunes propietats importants.

Proposició 2.1.2. *Siguin $a,b,c \in k^*$, aleshores*

(i) $(a,b) = (b,a)$.

(ii) $(a,b^2) = 1$.

(iii) $(a,-a) = 1$.

(iv) $(a,1-a) = 1$ *sempre que* $a \neq 1$.

(v) $(a,b) = (a,-ab) = (a,(1-a)b)$.

(vi) $(a,b) = 1 \implies (aa',b) = (a',b)$.

(vii) $(ac,b) = (a,b)(c,b)$.

Demostració. (i) És clar. En (ii) només hem d'observar el següent $z^2 - ax^2 - b^2y^2 = 0 \iff z^2 - ax^2 - (by)^2 = 0$ considerem la solució $(x, y, z) = (0, 1, b) \neq (0, 0, 0)$. (iii) És clar, doncs $z^2 - ax^2 + y^2 = 0$ té una solució no trivial $(x, y, z) = (1, 1, 0)$. Anàlogament, (iv) $z^2 - ax^2 - (1 - a)y^2 = 0$ té com a solució $(x, y, z) = (1, 1, 1) \neq (0, 0, 0)$. Provarem els punts restants més endavant en aquesta secció, de fet tots ells són casos especials de (vii). □

La propietat (vii) de fet ens diu que podem mirar el símbol de Hilbert com una aplicació de la següent manera

$$\begin{array}{ccc} k^*/(k^*)^2 \times k^*/(k^*)^2 & \longrightarrow & \{+1, -1\} \\ [a, b] & \longmapsto & (a, b). \end{array}$$

o bé, si anomenem

$$H_a = \left\{ b \in k^*; \quad \exists x, y \in k^* \quad b = x^2 - ay^2 \right\}$$

podem pensar en el següent morfisme de grups

$$\begin{array}{rccc} (a, \cdot): & k^* & \longrightarrow & \{+1, -1\} \simeq C_2 \\ & b & \longmapsto & (a, b) \end{array}$$

L'objectiu és demostrar que, efectivament, aquesta aplicació té nucli H_a, o equivalentment

$$k^*/H_a \simeq C_2.$$

Lema 2.1.3. *Per a tot $a \in k^*$ tenim que el conjunt*

$$H_a = \left\{ b \in k^*; \ \exists x, y \in k^* \quad b = x^2 - ay^2 \right\}$$

té estructura de grup multiplicatiu.

Demostració. Siguin $b, c \in H_a$, i siguin $x, y, z, t \in k$ tals que

$$\begin{cases} b = x^2 - ay^2 \\ c = z^2 - at^2. \end{cases}$$

Aleshores,

$$bc = (x^2 - ay^2)(z^2 - at^2) = x^2z^2 + a^2y^2t^2 - ay^2z^2 - ax^2t^2 = (xz + ayt)^2 - a(xt + yz)^2.$$

Ara, considerem

$$d = \left(\frac{x}{b}\right) - a\left(\frac{y}{b}\right)^2 \in H_a.$$

Aleshores, $bd = 1$, d'on $d = b^{-1}$, com volíem veure.

□

Lema 2.1.4. *Siguin $a, b \in k^*$ i a no és un quadrat, aleshores $(a, b) = 1$ si, i només si, $b \in H_a$.*

Demostració. Si $(a, b) = 1$ aleshores, existeixen $x_0, y_0, z_0 \in k$ no tots zero tals que $z_0^2 - ax_0^2 - by_0^2$, si y_0 fos zero tindríem $z_0^2 = ax_0^2$ i donat que ni x_0 ni z_0 poden anul·lar-se, tenim, que $a = \left(\frac{z_0}{x_0}\right)^2$, que és una contradicció. Per tant, $y_0 \neq 0$ i $b = \left(\frac{z_0}{y_0}\right)^2 - a\left(\frac{x_0}{y_0}\right)^2$.

Si $b \in H_a$, existeixen $x_0, z_0 \in k^*$ tals que $b = z_0^2 - ax_0^2$ i per tant, $(a, b) = 1$ ja que l'equació $z^2 - ax^2 - by^2 = 0$ té per solució $(x, y, z) = (x_0, 1, z_0)$. □

Teorema 2.1.5. *Si $a \in k^*$ no és un quadrat, aleshores $(k^* : H_a) = 2$.*

Sigui $p \neq 2$, aleshores $b \in H_a$ si, i només si, $z^2 - ax^2 - by^2 = 0$ té una solució. Vegem que existeixen elements de H_a que no són quadrats. Prenem $-a \in H_a$, si fos un quadrat l'equació $x^2 - ay^2$ és equivalent a $x^2 + y^2$, aleshores, si b és un element qualsevol de k^*, considerem $x^2 + y^2 - bz^2$, pel corol·lari del teorema de Chevalley-Warning (1.4.3) té una solució no trivial i per tant, $H_a = k^*$, però això no pot ser. Per tant, $k^{*2} \supsetneq H_a \supsetneq k^*$ i $(k^* : H_a) = 2$.

El cas $p = 2$ es pot veure de manera semblant, només s'han de considerar més casos, donat que les unitats de $\mathbb{Q}_2$ mòdul quadrats són $C_2 \times C_2 \times C_2$.

Corol·lari 2.1.6. *Per a $a, b, c \in k^*$ tenim que $(a, bc) = (a, b)(a, c)$.*

Demostració. Si $(a, b)(a, c) = -1$, o bé $(a, b) = -1$ i $(a, c) = 1$ o bé $(a, b) = 1$ i $(a, c) = -1$. Suposem sense pèrdua de generalitat que $(a, b) = -1$ i $(a, c) = 1$. Aleshores $c \in H_a$, si $(a, bc) = 1$ tindríem que $bc \in H_a$, però això implicaria $bcc^{-1} = b \in H_a$, per tant, $(a, bc) = -1$. Per simetria no cal considerar l'altre cas.

Suposem ara que $(a, bc) = -1$, tenim doncs que $bc \notin H_a$. Hem de veure que o bé $b \in H_a$ i $c \notin H_a$ o bé el contrari. Si els dos hi pertanyen, aleshores $bc \in H_a$ i $(a, bc) = 1$ que no pot ser. Suposem que cap dels dos hi pertany, aleshores $(a, b) = -1, (a, c) = -1$, pel lema anterior, la classe de bc en k^*/H_a és la classe del 1, per tant, $bc \in H_a$ i $(a, bc) = 1$. Com volíem veure. □

Corol·lari 2.1.7. $(a, a) = (a, -1)$.

Demostració. $(a, -a) = 1$, ja que $z^2 - ax^2 + ay^2 = 0$ té solució $(x, y, z) = (1, 1, 0)$. I pel teorema anterior, $(a, a) = (a, -1)(a, -a) = (a, -1)$. □

Teorema 2.1.8. *Si $k = \mathbb{R}$, $(a, b) = -1$ si, i només si, $a, b < 0$.*

Si $k = \mathbb{Q}_p$ per a algun primer p, escrivim $a = p^n u$ i $b = p^m v$, on u i v són unitats.

$$(a, b) = \begin{cases} (-1)^{nm\varepsilon(p)} \left(\frac{u}{p}\right)^m \left(\frac{v}{p}\right)^n & \text{si } p \neq 2, \\ (-1)^{\varepsilon(u)\varepsilon(v) + n\omega(v) + m\omega(v)} & \text{si } p = 2. \end{cases}$$

on llegim $\left(\frac{u}{p}\right)$ *com el símbol de Legendre de* $\psi_1(u)$ *sobre* p*. On* $\psi_1 : \mathbb{Z}_p \to \mathbb{F}_p$*. I* $\varepsilon(r) = \frac{r-1}{2}$ *i* $\omega(r) = \frac{r^2-1}{8}$ *mòdul 2.*

Demostració. Per bilinealitat només hem de veure els casos $(a,b) \in \{(p,u),(u,v)\}$ on u, v són unitats de $\mathbb{Z}_p$. Ja que

$$(p^n u, p^m v) = (p,p)^{nm}(u,p)^m(p,v)^n(u,v) = (p, u^m v^n (-1)^{nm})(u,v).$$

Suposem que $p \neq 2$, aleshores, calculem (p,u) on $u \in \mathbb{Z}_p^*$.

$$px^2 + uy^2 - z^2 = 0$$

té solució si, i només si, en té

$$ux^2 - z^2 = 0.$$

I això és cert si, i només si, u és un quadrat. Per tant, $(u,p) = \left(\frac{\overline{u}}{p}\right)$. D'altra banda, pel teorema de Chevalley-Warning i Hensel, l'equació

$$ux^2 + vy^2 - z^2 = 0$$

sempre té solució, d'on resulta $(u,v) = 1$.

Suposem ara que $p = 2$. Hem de determinar $(2,u),(u,v)$ per a $u, v \in Z_2^*$. Pel lema de Hensel sabem que

$$2x^2 + uy^2 - z^2 = 0$$

té solució si, i només si, $u \equiv 1 \pmod 8$, per tant, $(2,v) = (-1)^{\frac{v^2-1}{2}}$. L'equació

$$ux^2 + vy^2 - z^2 = 0$$

té solució si, i només si, almenys una unitat és congru amb 1 mòdul 4. Per tant, $(u,v) = (-1)^{\frac{u-1}{2}\frac{v-1}{2}}$.

□

2.2 Propietats globals

Donat que podem identificar $\mathbb{Q}$ com a subcòs de $\mathbb{Q}_p$ per a tot p, incloent-hi el primer de l'infinit i amb el conveni $\mathbb{Q}_\infty = \mathbb{R}$ denotarem per $(a,b)_p$ el símbol de Hilbert de les imatges de $a, b \in \mathbb{Q}^*$ en $\mathbb{Q}_p$.

Teorema 2.2.1 (Fórmula del producte)**.** *Siguin* $a, b \in \mathbb{Q}^*$*, aleshores tenim*

$$\prod_{p \text{ primer}} (a,b)_p = 1.$$

De fet, llevat d'un nombre finit de primers p *tenim que* $(a,b)_p = 1$*.*

Demostració. Si $a, b \in \mathbb{Q}^*$, aleshores, existeix una factorització de la següent manera

$$\begin{cases} a = \varepsilon p_1^{r_1} \cdots p_n^{r_n} \\ b = \eta q_1^{l_1} \cdots q_m^{l_m}. \end{cases}$$

On $\varepsilon, \eta \in \{\pm 1\}$, $r_1, \cdots, r_n, l_1, \cdots, l_m \in \mathbb{Z}$ i $p_1, \cdots, p_n, q_1, \cdots, q_m$ són primers.

De manera que, per a tot p primer

$$(a,b)_p = (\varepsilon, \eta)_p \prod_{i,j} (p_i, q_j)_p^{r_i l_j} \prod_i (p_i, \eta)_p^{r_i} \prod_j (\varepsilon, q_j)_p^{l_j}.$$

Com que $(1,1) = (1,-1) = (-1,1) = 1$, $(p_i, 1) = 1$ només hem de considerar els casos, en què a, b són -1 ambdós, dos nombres primers i un nombre primer i -1. Fent servir les fórmules que hem trobat en la secció de propietats locals.

Si $a = b = -1$, tenim que $(-1,-1)_p = -1$ si $p = 2, \infty$ i $(-1,-1)_p = 1$ en altre cas. El producte és 1.

Si $a = -1, b = q$ on q és un nombre primer. Si $q = 2$, $(-1,2)_p = 1$ per a tot p. Si $q \neq 2$, tenim $(-1,q)_p = 1$ si $p \neq 2, q$, i $(-1,q)_2 = (-1,q)_q = (-1)^{\frac{q-1}{2}}$, el producte torna a ser 1.

Si $a = q, b = l$ dos nombres primers, si $q = l$, tenim que $(q,q) = (q,-1)$ per tant ja està vist i podem considerar $q \neq l$. Si $q = 2$ tenim $(2,l)_p = 1$ sempre que $p \neq 2, l$ i $(2,l)_2 = (-1)^{\frac{l^2-1}{2}}$ i $(2,l)_l = \left(\frac{2}{l}\right) = (-1)^{\frac{l^2-1}{2}}$. Per tant, el producte és 1. Si ara cap dels dos és $= 2$, tenim que $(q,l)_p = 1$ si $p \neq 2, q, l$ i $(q,l)_2 = (-1)^{\frac{q-1}{2}\frac{l-1}{2}}$, $(q,l)_q = \left(\frac{l}{q}\right)$ i $(q,l)_l = \left(\frac{q}{l}\right)$. I per la llei de reciprocitat quadràtica,

$$\left(\frac{q}{l}\right)\left(\frac{l}{q}\right) = (-1)^{\frac{q-1}{2}\frac{l-1}{2}}.$$

D'on se segueix el resultat.

□

Teorema 2.2.2. *Sigui $\{a_i\}_{i \in I} \subset \mathbb{Q}^*$ on I és finit. I sigui $\{\varepsilon_{i,p}\}_{i \in I, p \in P}$, on P és el conjunt de nombres primers, i $\varepsilon_{i,p} = \pm 1$ per a tot $i \in I$. Per a que existeixin $x_i \in \mathbb{Q}^*$ tals que $(a_i, x_i)_p = \varepsilon_{i,p}$ per a tot subíndex és necessari i suficient que*

1. *Gairebé per tot i, p es tingui $\varepsilon_{i,p} = 1$.*
2. *Per a tot $i \in I$ es tingui $\prod_{p \in P} \varepsilon_{i,p} = 1$*
3. *Per a tot p primer existeixi $x_p \in \mathbb{Q}_p^*$ tal que $(a_i, x_p)_p = \varepsilon_{i,p}$ per a tot i.*

Demostrem primer el següent lema.

Lema 2.2.3. *Si P és un subconjunt finit de nombres primers, la imatge de $\mathbb{Q}$ dins de $\prod_{p\in P}\mathbb{Q}_p$ és densa.*

Demostració. Podem suposar que $\infty \in P$. Sigui $(x_0, x_1, \cdots, x_n) \in \mathbb{R}\times\mathbb{Q}_{p_1}\times\cdots\times\mathbb{Q}_{p_n}$. Podem suposar també que $(x_0,\cdots,x_n)\in\mathbb{R}\times\mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_n}$. Hem de provar que per a tot $\varepsilon>0$ i tot $N\in\mathbb{N}$ existeix $x\in\mathbb{Q}$ tal que $\mathrm{ord}_{p_i}(x-x_i)>N$ i $|x_0-x|<\varepsilon$, en virtut del teorema xinès dels residus existeix un enter y tal que $\mathrm{ord}_{p_i}(x-x_i)>N$ per a tot i, sigui q un nombre enter coprimer amb els p_i, escollim a tal que si $u=a/q^m$ per a un m prou gran

$$|y-x_0+up_1^N\cdots p_n^N|<\varepsilon,$$

per tant, el nombre buscat és $y+up_1^N\cdots p_n^N$. □

Demostrem doncs el teorema.

Demostració. Podem suposar sense pèrdua de generalitat que $\{a_i\}_{i\in I}\subseteq\mathbb{Z}$ (podem multiplicar per quadrats enters). Sigui S el subconjunt de P tal que conté els factors primers de a_i i $2,\infty$. Sigui T el conjunts dels primers p tals que existeix $i\in I$ tal que $\varepsilon_{i,p}=-1$. Aquests dos conjunts són finits. Distingim dos casos:

- Si posem $S\cap T=\varnothing$. Sigui

$$a=\prod_{p\in T\setminus\{\infty\}}p \quad \text{i} \quad m=8\prod_{p\in S\setminus\{2,\infty\}}p.$$

  Com que $S\cap T=\varnothing$ tenim que $\mathrm{mcd}(a,m)=1$. El Teorema de Dirichlet ens diu que si s,t són dos nombres coprimers, aleshores existeixen infinits primers p tals que $p\equiv t \pmod s$. En conseqüència, existeix almenys un primer q tal que $q\equiv a \pmod m$ i $q\notin S\cup T$. Provarem que $x=aq$ té la propietat desitjada, és a dir, $(a_i,x)_p=\varepsilon_{i,p}$ per a tot $i\in I$ i $p\in P$.

  Si $p\in S$, aleshores $\varepsilon_{i,p}=1$, ja que $S\cap T=\varnothing$ i volem veure que $(a_i,x)_p=1$. Si $p=\infty$ el resultat és clar ja que $x>0$. Si p és un primer finit, tenim que $x\equiv a^2 \pmod m$, per tant $x\equiv a^2 \pmod 8$ per a $l=2$ i $x\equiv a^2 \pmod l$ per a $l\neq 2$, com que a són unitats l-àdiques, això demostra que x és un quadrat en $\mathbb{Q}_l^*$ de manera que $(a_i,x)_p=1$.

  Si $p=l$ no està en S, a_i és una unitat l-àdica. Com que $l\neq 2$ tenim

$$(a_i,b_i)=\left(\frac{a_i}{l}\right)^{\mathrm{ord}_l(b)},$$

  per a tot $b\in\mathbb{Q}_l^*$. Si $l\notin T\cup\{p\}$, x és una unitat l-àdica ja que $\mathrm{ord}_l(x)=0$ i la fórmula mostra que $(a_i,x)_l=1$; i a més a més $\varepsilon_{i,l}=1$ ja que $l\notin T$. Si $l\in T$ tenim $\mathrm{ord}_l(x)=1$, a més a més, la condició 3 mostra que existeix $x_l\in\mathbb{Q}_l^*$ tal

que $(a_i, x_l)_l = \varepsilon_{i,l}$ per a tot $i \in I$, donat que un dels $\varepsilon_{i,l} = -1$ tenim $\mathrm{ord}_l(x_l) \equiv 1 \pmod 2$ d'on

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l},$$

per a tot $i \in I$. Només queda el cas $l = p$, i el deduïm dels altres fent servir que

$$(a_i, x)_q = \prod_{p \neq q} (a_i, x)_p = \prod_{p \neq q} \varepsilon_{i,q}.$$

- Sabem que els quadrats de $\mathbb{Q}_p^*$ formen un subgrup obert de Q_p^*, pel lema 2.2.3, existeix $x' \in \mathbb{Q}^*$ tal que x'/x_v és un quadrat en $\mathbb{Q}_p^*$ per a tot $p \in S$, en particular $(a_i, x')_p = (a_i, x_p)_p = \varepsilon_{i,p}$ per a tot $p \in S$. Si posem $\eta_{i,p} = \varepsilon_{i,p}(a_i, x')_p$, aquesta família verifica les condicions 1,2 i 3 del teorema que estem demostrant i a més a més $\eta_{i,p} = 1$ si $p \in S$. Pel cas anterior, existeix $y \in Q^*$ que compleix $(a_i, y)_p = \eta_{i,p}$ per a tot $i \in I$ i $p \in P$. Si posem $x = yx'$ és clar que x compleix el que volem.

□

Capítol 3

Formes quadràtiques

Aquest capítol, juntament amb el següent, és el nucli del nostre treball. Fem un estudi exhaustiu dels espais quadràtics. Introduïm el concepte *local-global* i estudiem la seva aplicació en aquests espais.

3.1 Definicions i propietats

Definició 3.1.1. *Sigui A un anell commutatiu. Una forma quadràtica és un polinomi homogeni $Q \in A[X_1, \cdots, X_n]$ de grau 2.*

Ens centrarem en el cas en què A és un cos de característica diferent de 2 que notarem d'ara endavant com a k.

Podem expressar qualsevol forma quadràtica de la següent manera

$$Q(X_1, \cdots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j$$

i podem considerar la matriu de coeficients M_Q definida per

$$M_Q = (m_{ij})_{ij} = \begin{cases} m_{ii} = a_{ii} \quad \text{per a tot } i, \\ m_{ij} = m_{ji} = \frac{1}{2} a_{ij}. \end{cases}$$

Aquest és un mètode natural de considerar una matriu simètrica que compleix que si $v = (X_1, \cdots, X_n)^t$ tenim que $v^t M_Q v = Q$.

Si efectuem un canvi de base dins el un espai vectorial V de dimensió n per una matriu B que ha de ser invertible, obtenim una nova matriu M'_Q que ens defineix la mateixa forma quadràtica. I donat que $M_Q = B M'_Q B^t$, tenim

$$\det(M_Q) = \det(M'_Q) \det(B)^2,$$

i el determinant de la matriu M_Q queda precisat unívocament en $k^*/(k^*)^2$.

Definició 3.1.2. *Sigui Q una forma quadràtica sobre un cos k. Sigui M_Q la seva matriu associada. Anomenem discriminant de Q al determinant de M_Q mòdul els quadrats de k^*, ho escrivim* $\mathrm{disc}(Q)$.

Una manera de veure les formes quadràtiques és la següent. Sigui A un anell commutatiu i V un A-mòdul. Anomenarem forma quadràtica a tota funció $Q : V \longrightarrow A$ tal que

(i) $Q(ax) = a^2Q(x)$ per a tot element $a \in A$.

(ii) L'assignació $(x, y) \longmapsto Q(x + y) - Q(x) - Q(y)$ és una forma bilineal.

Aleshores, anomenem a (V, Q) mòdul quadràtic. Amb les condicions anteriors hem de suposar que A és un cos k i que V és un k-espai vectorial de dimensió finita. Direm que V és un espai quadràtic de forma quadràtica Q.

Definició 3.1.3. *Diem que una forma quadràtica Q en les variables $X_1, \cdots, X_n$ a coeficients en k un cos representa $a \in k$, si existeix, $(a_1, \cdots, a_n) \in k^n$ tal que $Q(a_1, \cdots, a_n) = a$.*

Per a poder classificar les formes quadràtiques necessitem veure com les podem escriure de manera general i simple.

En general, si $Q \in k[X_1, \cdots, X_n]$ és una forma quadràtica, l'assignació de la seva matriu M_Q ens porta de manera directa a l'estudi de l'espai vectorial associat V de dimensió n amb la *mètrica* induïda pel *producte escalar* següent

$$x \cdot y = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

Aquesta definició és natural, doncs, si ho escrivim en forma matricial, el que obtenim és que

$$x \cdot y = x^t M_Q y.$$

I donat que suposem que la característica és diferent de 2 podem afirmar que es tracta d'una forma bilineal.

Observació 3.1.4. *Hem de tenir en compte que no es tracta d'un producte escalar i tampoc indueix cap mètrica en general. El cas que ens ocupa és el de formes quadràtiques en general, i les que volem estudiar són aquelles que són no definides positives. Si ho fossin no tindríem solucions a les equacions plantejades. Emperò, filosòficament parlarem de morfismes mètrics i de producte escalar per a simplificar la notació.*

Definició 3.1.5. *Si Q és una forma quadràtica V el seu espai vectorial, n la seva dimensió i $x, y \in V$, diem que x, y són ortogonals si, i només si,*

$$x \cdot y = 0.$$

Si $G \subseteq V$ és un subespai vectorial, definim el seu ortogonal com

$$G^{\perp} := \{x \in k^n; \quad x \cdot y = 0 \quad \forall y \in G\}.$$

Si $G_1, \cdots, G_n$ són subespais vectorials de V, diem que V és la suma directa ortogonal dels subespais G_i si són ortogonals dos a dos i V és la suma directa d'aquests subespais. En aquest cas escrivim

$$V = G_1 \perp \cdots \perp G_n.$$

Sigui $\{e_1, \cdots, e_n\}$ una base. Diem que és una base ortogonal si V és la suma directa ortogonal de $\langle a_1 \rangle, \cdots, \langle a_n \rangle$. On $a_i = Q(e_i)$.

Definició 3.1.6. *Sigui V un espai quadràtic i Q la seva forma quadràtica. Diem que V és no degenerat si $V^{\perp} = 0$ i que és degenerat si existeix un vector no nul $x \in V^{\perp}$. Definim el seu rang com* $\operatorname{rank}(Q) = n - \dim(V^{\perp})$.

Teorema 3.1.7. *Sigui V un espai quadràtic de forma quadràtica Q de dimensió n. Aleshores existeix una base ortogonal respecte al producte escalar definit en 3.1.5.*

Observació 3.1.8. *De fet, el què busquem és una diagonalització de la matriu associada a Q.*

Demostració. Ho provarem per inducció en n i suposem que Q no representa 0, si no el resultat és clar. Si $n = 1$, tenim que només hi ha un vector linealment independent i el resultat és clar. Per a $n > 1$ escollim $e_1 \in V$ tal que $Q(e_1) \neq 0$, aleshores tenim $G = \langle e_1 \rangle^{\perp}$ és un hiperplà i $e_1 \neq G$ ja que no és isotròpic, $\dim G = n - 1$ i per hipòtesi d'inducció obtenim el resultat. □

Observació 3.1.9. *En aquest punt és clar que la condició de no degeneració és equivalent a què la matriu associada a Q no tingui cap valor propi igual a 0.*

Observació 3.1.10. *Aquest resultat és important donat que ens permet caracteritzar els espais i les formes quadràtiques de forma eficient. De fet, la conseqüència més directa és l'existència d'una base en la què la matriu de Q és diagonal. Això ens permet dir que per a una certa base Q es pot escriure com*

$$Q(X_1, \cdots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2.$$

I per tant, $d(Q) = a_1 \cdots a_n$.

L'aplicació principal del teorema següent és la caracterització dels morfismes mètrics d'un espai vectorial en un altre i d'aquesta manera estudiar els isomorfismes entre ells.

Teorema 3.1.11 (Witt). *Siguin V i V' dos espais quadràtics amb formes quadràtiques Q i Q' respectivament. Suposem que V i V' són no degenerats, que tenen la mateixa dimensió i que existeix un morfisme de V en V' que transforma Q en Q'. Aleshores, tot morfisme injectiu i mètric (i.e. respecta el producte escalar de Q)*

$$f : G \longrightarrow V',$$

on G és un subespai vectorial de V pot ser estès en un morfisme mètric.

Demostració. Suposem primer que G és un subespai vectorial no degenerat respecte a Q.

Vegem-ho per inducció completa. Si $\dim G = 1$ donat que G és no degenerat existeix un element x no isotròpic. Donat que f és mètric $f(x) \cdot f(x) = x \cdot x$, definim $y = f(x)$. Ara, o bé $x + y$ o bé $x - y$ és no isotròpic. Si ho fossin tindríem

$$Q(x + y) = 0 = Q(x - y)$$

Observem que $Q(z) = z \cdot z$, així doncs

$$\begin{aligned}(x + y) \cdot (x + y) &= 0 = (x - y) \cdot (x - y)\\ x \cdot x + 2x \cdot y + y \cdot y &= 0 = x \cdot x - 2x \cdot y + y \cdot y\\ 2x \cdot x + 2x \cdot y &= 0 = 2x \cdot x - 2x \cdot y\\ 4x \cdot y &= 0\\ x \cdot y &= 0.\end{aligned}$$

on suposem que la característica de k no és 2. Suposar això no és quelcom greu ja que en general treballarem amb cossos de característica 0 ($\mathbb{Q}$ i $\mathbb{Q}_p$). Ara, si $x \cdot y = 0$ de l'equació anterior obtenim $Q(x) = x \cdot x = 0$ però això no pot ser.

Sigui $\varepsilon = \pm 1$ tal que $x + \varepsilon y$ és no isotròpic. Sigui $H = \langle x + \varepsilon y \rangle^{\perp}$, d'on $k^n = \langle x + \varepsilon y \langle \hat{\oplus} H$. Sigui g el morfisme que deixa invariant H i tal que $g(x + \varepsilon y) = -x - \varepsilon y$. Donat que $x - \varepsilon y \in H$ es té $g(x - \varepsilon y) = x - \varepsilon y$ i $g(x + \varepsilon y) = -x - \varepsilon y$ en deduïm que $g(x) = -\varepsilon y$ per tant, $-\varepsilon g$ estén f.

Si $\dim G > 1$ podem descompondre $G = G_1 \perp G_2$ no trivialment per hipòtesi d'inducció la restricció de f a G_1 estén a un morfisme, canviant f per $g^{-1} \circ f$ si cal podem suposar que f és la identitat en G_1 i per hipòtesi d'inducció de nou podem estendre a partir de G_2.

Ara, si G és degenerat podem estendre f a un morfisme injectiu i mètric de G' en V' on G és hiperplà de G'.

Sigui $x \in U^{\perp}$ no nul i h una forma lineal tal que $h(x) = 1$, com que V' és no degenerat, existeix $y \in V'$ tal que $h(z) = z \cdot y$ per a tot z. Sense pèrdua de generalitat podem suposar $y \cdot y = 0$, ara $G' = G \perp \langle y \rangle$ conté G com a hiperplà, ara podem fer la mateixa construcció amb la imatge de G per f i estenem així f.

□

3.2 Isotropia

Definició 3.2.1. *Sigui V un espai quadràtic amb Q la seva forma quadràtica, sigui n la dimensió de V. Diem que $x \in V$ és isotròpic si $Q(x) = 0$, diem que és anisotròpic si $Q(x) \neq 0$. En particular, si G és un subespai vectorial, diem que G és isotròpic si conté un element isotròpic altrament és anisotròpic. Diem que és totalment isotròpic si tots els seus vectors no nuls són isotròpics.*

Un exemple d'espai isotròpic és el pla hiperbòlic.

Definició 3.2.2. *Sigui k un cos, V un k-espai vectorial quadràtic de dimensió 2 i $Q \in k[X,Y]$ la seva forma quadràtica tal que en una certa base $V = \langle 1 \rangle \perp \langle -1 \rangle$. Diem que V és el pla hiperbòlic.*

Definició 3.2.3. *Sigui V un k-espai vectorial quadràtic. Definim el seu radical com*

$$\mathrm{rad}(V) := V \cap V^{\perp}.$$

Aleshores, diem que V és regular si

$$\mathrm{rad}(V) = 0.$$

Proposició 3.2.4. *Sigui V un espai vectorial quadràtic de dimensió 2 i sigui Q la seva forma quadràtica associada. Les següents afirmacions són equivalents.*

(i) V *és el pla hiperbòlic.*

(ii) V *és isotròpic i regular.*

(iii) $d(Q) = -1$.

Demostració. 1. $(i) \implies (ii)$ La matriu del pla hiperbòlic és

$$M_Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Per tant, si fem,

$$\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 - 1 = 0.$$

Per tant, és isotròpic. Vegem que és regular.

Sigui $v \in V^{\perp}$, aleshores, $v = (x,y)$ i $v^t M_Q u = 0$ per a tot $u \in V$, en particular, $x + y = 0$ i $x - y = 0$, d'on $v = (0,0)$ i V regular.

2. $(ii) \implies (iii)$. Sigui x un vector isotròpic, estenem-lo a una base, la matriu de Q en aquesta base és
$$\begin{pmatrix} 0 & \beta \\ \beta & \gamma \end{pmatrix},$$
per tant, $d(Q) = -\beta^2$, donat que V és regular $\beta \in k^*$ i $d(Q) \equiv -1 \pmod{k^{*2}}$.

3. $(iii) \implies (i)$. Com que $d(Q) \neq 0$ tenim que $Q(V) \neq 0$ per tant V és regular. Sigui $a \in Q(V)$ i sigui x tal que $Q(x) = a$, per regularitat, existeix y tal que $V = \langle x \rangle \perp \langle y \rangle$. $d(Q) = -1 \implies -Q(x)Q(y)$ és un quadrat no nul, podem suposar $Q(y) - a$ i per tant en aquesta base la matriu és la que defineix el pla hiperbòlic.

□

Lema 3.2.5. *Sigui V un espai quadràtic regular i Q la seva forma quadràtica, sigui α un escalar. Aleshores, $\alpha \in Q(V)$ si, i només si, $\langle -\alpha \rangle \perp V$ és isotròpic.*

Demostració. Considerem l'espai $W = \langle z \rangle \perp V$ amb $Q(z) = -\alpha$, si existeix x tal que $Q(x) = \alpha$ tenim que $Q(x + y) = 0$ i per tant W és isotròpic. Recíprocament, si V és isotròpic aleshores representa tot element de k i si no és isotròpic ha d'haver un escalar no nul β i un vector $y \in V$ tal que $Q(\beta z + y) = 0$, però aleshores $-\beta^2\alpha + Q(y) = 0$, per tant, $\alpha \in Q(y)/\beta^2 \in Q(E)$. □

Proposició 3.2.6. *Sigui $U \subseteq V$ dos espais vectorials quadràtics de dimensions 3 i 4 respectivament. Sigui Q la seva forma quadràtica associada i suposem que $d(Q) = 1$. Aleshores, V és isotròpic si, i només si, U és isotròpic.*

Demostració. Ara, pel lema anterior, escrivim $V = U \perp \langle \alpha \rangle$ amb α no nul, per tant, $-\alpha \in Q(U)$ i $U = P \perp \langle -\alpha \rangle$ on P és un pla, per tant, $V = P \perp \langle -\alpha \rangle \perp \langle \alpha \rangle$ i $d(V) = 1 = -d(P)$ per tant, $d(P) = -1$ i pel que hem vist és el pla hiperbòlic, per tant U és isotròpic. □

Proposició 3.2.7. *Sigui V un espai quadràtic regular de dimensió 4 i d el seu discriminant. Sigui $K = k(\sqrt{d})$. Aleshores, V és isotròpic si, i només si, KV és isotròpic.*

Observació 3.2.8. *Ens referim a KV com l'espai generat pels mateixos vectors però sobre K. És a dir, si*
$$V = \langle e_1, \cdots, e_s \rangle,$$
$$KV = \{ v = k_1 e_1 + \cdots + k_s e_2; \quad k_i \in K \text{ per a tot } i \}.$$

Demostració. Com que $V \subseteq KV$, la necessitat és clara. Vegem la suficiència. Sigui KV un espai isotròpic i suposem que V no és isotròpic. Aleshores $\operatorname{disc}(Q)$ no és cap quadrat en k i $K|k$ és quadràtica, per tant tot element és de la forma $x + y\sqrt{d}$. Sigui $x + y\sqrt{d}$ un element isotròpic de KV. Aleshores,
$$Q(x) + dQ(y) + 2\sqrt{d}(x \cdot y) = 0.$$

D'on se segueix que $Q(x) = -dQ(y)$ i $x \cdot y = 0$. Si $Q(y) = 0$ tenim que $Q(x) = 0$, i per tant $x = y = 0$ ja que suposem que V no conté elements isotròpics. Però això implicaria que $x + y\sqrt{d}$ no seria isotròpic. Per tant posem $Q(y) = \varepsilon \neq 0$, $Q(x) = -d\varepsilon$, $x \cdot y = 0$. Ara,

$$V \simeq \langle \varepsilon \rangle \perp \langle -d\varepsilon \rangle \perp P.$$

El discriminant és doncs $\operatorname{disc}(Q) = -d\varepsilon^2 \operatorname{disc}(Q|_P) = -d\operatorname{disc}(Q|_P)$ en k^*/k^{*2}. Però $\operatorname{disc}(Q) = d$, per tant, $\operatorname{disc}(Q|_P) = -1$. Per la proposició 3.2.4, com que $\operatorname{rank}(Q|_P) = 2$ tenim que P és el pla hiperbòlic, i en conseqüència V és isotròpic. □

3.3 Invariants i classificació

En general per a fer la classificació introduirem tres invariants, dos dels quals ja s'han vist.

En primer lloc tenim el rang d'una forma quadràtica. Se segueix de la definició que no depèn de cap base. En segon lloc tenim el discriminant que també és invariant. I en tercer lloc tenim el següent

Definició 3.3.1. *Sigui V un espai quadràtic, Q la seva forma quadràtica i sigui $e = \{e_1, \cdots, e_n\}$ una base ortogonal. Escrivim*

$$V = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle,$$

on $a_i = Q(e_i)$. Definim

$$\varepsilon(e) = \prod_{i<j} (a_i, a_j) \in \{1, -1\},$$

on, per a tot i, j (a_i, a_j) denota el símbol de Hilbert de a_i i a_j en el cos k.

Proposició 3.3.2. *Sota les mateixes condicions, $\varepsilon(e)$ no depèn de la base e.*

Demostració. Cf. [13]. □

Observació 3.3.3. *En general escriurem $\varepsilon(Q)$ (o ε si la referència a Q és clara) en comptes de referir-nos a la base.*

Definició 3.3.4. *Siguin V i V' dos espais quadràtics i Q i Q' les seves formes quadràtiques respectivament en n i m les dimensions respectives. Direm que Q i Q' són equivalents si hi ha un isomorfisme entre V i V' que transformi Q en Q'. Ho escriurem $Q \sim Q'$.*

Observació 3.3.5. *En particular, si dues formes són equivalents representen els mateixos elements.*

Per a poder classificar les formes quadràtiques abans de tot hem de veure quan aquestes formes representen 0.

Proposició 3.3.6. *Sigui p un primer (inclòs el primer de l'infinit) i sigui V un k-espai vectorial quadràtic de forma quadràtica Q, r el seu rang, d el seu discriminant i $\varepsilon = \varepsilon(Q)$. V és isotròpic si, i només si es compleix alguna de les condicions següents:*

1. *$r = 2$ i $d = -1$ en k^*/k^{*2}.*
2. *$r = 3$ i $(-1, -d) = \varepsilon$.*
3. *$r = 4$ i*
   - *$d \neq 1$ o bé,*
   - *$d = 1$ i $\varepsilon = (-1, -1)$.*
4. *$r \geq 5$.*

Demostració. Podem escriure V com

$$V = \langle a_1 \rangle \perp \cdots \perp \langle a_r \rangle$$

en una base adequada.

1. Si $r = 2$ podem escriure $Q = ax^2 + by^2$, aquesta forma representa zero si, i només si, $-b/a$ és un quadrat, com que k^{*2} és grup multiplicatiu, $(-b/a)a^2 = -ba = -d$ és un quadrat, en particular, $-d \equiv -1 \pmod{k^{*2}}$.

2. Si $r = 3$ podem posar $Q = ax^2 + by^2 + cz^2$ i podem suposar $c = 1$ (podem multiplicar per c i com que es un quadrat en k^* tenim les mateixes solucions que és el què busquem). Per tant, $Q = ax^2 + by^2 + z^2$, i això és equivalent a què $(-a, -b) = 1$, desenvolupant trobem que és necessari i suficient que:

$$\begin{aligned} 1 &= (-1,-1)(-1,b)(a,-1)(a,b) \\ 1 &= (-1,b)(-1,a)(a,b) \\ 1 &= (-1,ab)(a,b)(a,1)(b,1) \\ 1 &= (-1,d)\varepsilon \\ \varepsilon &= (-1,d). \end{aligned}$$

   On en la tercera igualtat fem servir que $1 \in k^{*2}$ i per tant $(1, a) = (1, b) = 1$.

3. Si $r = 4$, podem escriure $Q = ax^2 + by^2 + cz^2 + eu^2$. És equivalent que Q representi a 0 i què $ax^2 + by^2$ i $-cz^2 - eu^2$ representin un element $t \in k^*/k^{*2}$. Per tant, això equival pel cas $r = 2$ a dir que $(t, -ab) = (a, b)$ i $(t, -ce) = (c, e)$

4. Demostrem el cas $r = 5$. Sigui

$$V = \langle a_1 \rangle \perp \cdots \perp \langle a_5 \rangle$$

una descomposició perpendicular de V, en una base adequada. Escalant si cal, podem suposar que dos d'ells són diferents mòdul k^{*2}, i per tant, diferents de d. Aleshores, descomponem V com

$$V = \langle a \rangle \perp W,$$

amb W un subespai de rang 4. Aleshores, el discriminant de la forma $Q|_W$ és $d(Q|_W) = d/a \neq 1$. Per tant, pel cas $r = 4$ W és isotròpic, com que $W \subseteq V$ per a qualsevol element isotròpic hi ha un element isotròpic en V (agafem les coordenades corresponents a W iguals i la coordenada que hi manca igualada a 0). El cas $r > 5$ és trivial, doncs $V = W \perp H$, on W és de rang 5, i pel ,mateix raonament, V és isotròpic. El cas $p = \infty$ és clar.

□

Teorema 3.3.7. *Siguin Q i Q' dues formes quadràtiques sobre k són equivalents si, i només si, tenen el mateix rang, discriminant i ε.*

Demostració. La necessitat és clara. Vegem la suficiència. Ho provarem per inducció en el rang n. El cas $n = 0$ és trivial. De la proposició 3.3.6 se segueix que si Q i Q' tenen els mateixos invariants representen els mateixos elements en k^*/k^{*2}. Sigui doncs $a \in k^*$ representat per ambdues formes alhora. Podem escriure

$$Q = aZ^2 + H, \quad Q' = aZ^2 + H'.$$

Les formes H, H' són de rang $n-1$. A més a més,

$$d(H) = ad(Q) = ad(Q') = d(H').$$

$$\varepsilon(H) = \varepsilon(Q)(a, d(H)) = \varepsilon(Q')(a, d(H')) = \varepsilon(H').$$

Per hipòtesi inductiva, $H \sim H'$, per tant, $Q \sim Q'$. □

3.4 El principi de Hasse

El principi de Hasse deu el seu nom al matemàtic Helmut Hasse (1898-1979) que va ser un dels primers matemàtics que estudià les aplicacions dels nombres p-àdics en la teoria de nombres. Un dels noms que rep aquest principi és el de local-global, ja que la filosofia intrínseca és comparar el comportament de certes equacions diofantines en $\mathbb{Q}$ o en $\mathbb{Z}$ i en els seus localitzats. Diem que una solució en $\mathbb{Q}$ i $\mathbb{Z}$ és global ja que implica una solució en tot $\mathbb{Q}_p$.

El nostre objectiu principal en aquesta secció és demostrar el teorema de Hasse-Minkowski, que és el següent

Teorema 3.4.1 (Hasse-Minkowski)**.** *Sigui Q una forma quadràtica sobre $\mathbb{Q}$, aleshores Q representa 0 si, i només si, Q representa 0 en $\mathbb{Q}_p$ per a tot p primer.*

Farem una demostració ajudant-nos de la teoria que hem desenvolupat d'espais isotròpics.

En aquesta secció V serà un espai vectorial quadràtic de dimensió n, denotarem el seu producte escalar com hem fet en la resta del capítol i la forma quadràtica que indueix el producte escalar serà representada per Q. Per a tot p primer de $\mathbb{Z}$, denotarem per V_p el localitzat de V, és a dir, l'espai vectorial engendrat pels mateixos vectors però dins de $\mathbb{Q}_p$.

Teorema 3.4.2 (Hasse-Minkowski)**.** *Sigui V un k-espai vectorial regular sobre $\mathbb{Q}$. Aleshores, V és isotròpic si, i només si, V_p és isotròpic per a tot p primer de $\mathbb{Z}$.*

Demostració. Només hem de mostrar la suficiència. Suposem que $n \geq 2$, el cas 1 no té sentit. Suposem, a més a més, que V_p és isotròpic, és a dir, conté un element isotròpic per a tot p. Sigui $e = \langle e_1, \cdots, e_n \rangle$ una base de V tal que

$$V = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$$

en aquesta base.

Fem-ho per casos

- $n = 2$, pel que hem vist anteriorment, $d(Q_p) = -1$, és a dir $-a_1a_2 \in \mathbb{Q}_p^2$ per a tot p. Per tant, és un quadrat de $\mathbb{Q}$ i $d(Q) = -1$ d'on se segueix que V és el pla hiperbòlic i per tant és isotròpic.

- $n = 3$ Escalant si cal, podem suposar que V té una descomposició

  $$V = L \perp P,$$

  on $L = \langle -\alpha \rangle$ i $P = \langle 1 \rangle \perp \langle -\theta \rangle$. Podem suposar a més a més que θ és lliure de quadrats en $\mathbb{Q}$. Siguin L_p i P_p les localitzacions naturals dins de V_p. Donat que V_p és isotròpic per hipòtesi, sabem pel lema 3.2.5 que P_p representa α en tot p per tant en pel cas anterior $\mathbb{Q}$, així l'equació

  $$\alpha = x_p^2 - \theta y_p^2$$

  té solució per a tot p on $x_p, y_p \in \mathbb{Q}_p$. Sigui $m = |\alpha| + |\theta|$, si $m = 2$ el resultat és clar. Suposem $m > 2$, en particular $|\theta| \geq 2$. Sigui

  $$\theta = \pm p_1 \cdots p_k,$$

  amb $p_i \neq p_j$ si $i \neq j$. Hem vist que α és un quadrat mòdul $p = p_i$, ja que α és una norma de $\mathbb{Q}(\sqrt{\theta})$. Per tant, θ és un quadrat mòdul θ. D'on se segueix que existeixen t, r tals que

  $$t^2 = \alpha + \theta r.$$

Escollim t tal que $|t| \leq \frac{|\theta|}{2}$. Ara, $\theta r = t^2 - \alpha$ ens diu que θr és una norma de $k(\sqrt{\alpha})|k$, on k és un p-àdic o $\mathbb{Q}$. D'això concloem que la nostra forma quadràtica representa 0 si, i només si, la forma

$$Q' = Z^2 - \alpha X^2 - rY^2$$

representa 0.

En particular, Q' representa 0 en tot p-àdic. Ara,

$$|r| = \left|\frac{t^2 - \alpha}{b}\right| \leq \frac{|\theta|}{4} < |\theta|.$$

Ja que $|\theta| \geq 2$. Escrivim $r = r'u^2$, de manera que r' sigui lliure de quadrats. Tenim que $|r'| < |\theta|$, i apliquem hipòtesi d'inducció a la forma

$$Q'' = Z^2 - \alpha X^2 - r'Y^2 \sim Q'$$

Per tant, V' és isotròpic, i per tant, V és isotròpic.

- $n = 4$ Suposem primer que el discriminant de Q és 1, sigui U un subespai regular ternari de V. Ara, V_p és isotròpic per a tot p, per tant U_p també ho és, per tant, per la proposició 3.2.6 tenim que U_p és isotròpic, ara pel cas $n = 3$ es té que U és isotròpic. Per tant, de nou per la proposició 3.2.6 V és isotròpic. Considerem el cas on $d(Q) \neq 1$, sigui $K = \mathbb{Q}(\sqrt{a_1a_2a_3a_4})$ l'extensió quadràtica que s'obté d'afegir l'arrel quadrada del discriminant. I considerem, per a tot $\mathfrak{p}$ primer de l'anell d'enters de K l'espai vectorial

$$(KV)_{\mathfrak{p}} = \langle a_1 \rangle_{K_{\mathfrak{p}}} \perp \cdots \perp \langle a_4 \rangle_{K_{\mathfrak{p}}}$$

que conté

$$\langle a_1 \rangle_{\mathbb{Q}_{\mathfrak{p}}} \perp \cdots \perp \langle a_4 \rangle_{\mathbb{Q}_{\mathfrak{p}}}.$$

I aquest espai es isotròpic perquè

$$V_p = \langle a_1 \rangle_{\mathbb{Q}_p} \perp \cdots \perp \langle a_4 \rangle_{\mathbb{Q}_p}$$

és isotròpic en la localització p induïda per $\mathfrak{p}$ en $\mathbb{Q}$. Per tant, $(KV)_{\mathfrak{p}}$ és isotròpic per a tot primer $\mathfrak{p}$ de K. $d(EV) = 1$, d'on se segueix que EV és isotròpic, i obtenim que V és isotròpic per la proposició 3.2.7.

- $n \geq 5$. Ho demostrarem per inducció sobre n. Suposem $n \geq 5$, sigui

$$U = \langle a_1 \rangle \perp \langle a_2 \rangle, \quad W = \langle a_3 \rangle \perp \cdots \perp \langle a_n \rangle,$$

de manera que $V = U \perp W$. Prenem les localitzacions U_p, W_p dins de V_p i sigui

$$T = \{p \text{ primer } ; W_p \text{ anisotròpic } \}.$$

El conjunt és finit pel que hem vist fins ara. Efectivament, només cal veure que $Q|_W$ té 3 variables mínim, pel Teorema de Chevalley-Warning (1.4.3) i Hensel (1.3.6), sabem que $Q|_{W_p}$ té solució sempre que p no divideixi $x_3, \cdots, x_n$ o, en alguns casos 2, és a dir, pel teorema fonamental de l'aritmètica, aquestes excepcions són finites.

Si T és buit, tenim que W és isotròpic per hipòtesi d'inducció i ja estaríem. Considerem doncs, $T \neq \varnothing$ un conjunt finit. Aleshores, existeix $\mu_p \in \mathbb{Q}_p^*$ per a tot p primer en T tal que

$$\mu_p \in Q(U_p), \quad -\mu_p \in Q(W_p)$$

si U_p no és isotròpic és perquè V_p és isotròpic, en altre cas seria una conseqüència de la universalitat dels plans hiperbòlics. Per tant, tenim $\eta_p, \xi_p \in \mathbb{Q}_p$ en tot $p \in T$ tal que

$$Q(\xi_p x_1 + \eta_p x_2) = \xi_p^2 a_1 + \eta_p^2 a_2 = \mu_p.$$

Podem trobar ara $\xi, \eta \in \mathbb{Q}$ prou propers a ξ_p, η_p respectivament per a tot $p \in T$ (ja que és finit). Sigui $\mu = Q(\xi x_1 + \eta x_2)$. Prenent una bona aproximació, podem fer que μ sigui prou proper a μ_p per a tot $p \in T$, i podem fer $|\mu\mu_p^{-1} - 1|_p$ tan petit com vulguem per a tot $p \in T$. Com que $\mathbb{Q}_p^{*2}$ és un obert de $\mathbb{Q}_p$ podem obtenir $\mu' \in \mu_p \mathbb{Q}_p^{*2}$ per a tot $p \in T$. Donat que $\xi x_1 + \eta x_2$ està en U tenim que

$$V \simeq \langle \mu' \rangle \perp \langle \mu \rangle \perp W.$$

Per tant, $\langle \mu \rangle \perp W$ és isotròpic ja que $-\mu \in -\mu_p \mathbb{Q}_p^{*2}$, i és isotròpic en la resta de p que no estan en T. En conseqüència ho és V.

□

Teorema 3.4.3. *Sigui E un espai vectorial quadràtic de dimensió n, aleshores E és isotròpic sempre que $n \geq 5$ i sigui isotròpic sobre $\mathbb{R}$.*

Demostració. Hem vist en la proposició 3.3.6 que tot espai V de rang 5 és isotròpic en tot localitzat, i pel teorema de Hasse-Minkowski V és isotròpic sobre $\mathbb{Q}$. □

Proposició 3.4.4. *Sigui V un espai quadràtic de dimensió 3 i sigui q un nombre primer (incloent-hi el primer de l'infinit). Si V_p és isotròpic per a tot $p \neq q$, aleshores V és isotròpic en $\mathbb{Q}$.*

Demostració. Sigui

$$V = \langle a \rangle \perp \langle b \rangle \perp \langle c \rangle.$$

El resultat és trivial si $abc = 0$. Per la proposició 3.3.6 V_p és isotròpic si, i només si,

$$(-1, -abc)_p = (a, b)_p (a, c)_p (b, c)_p.$$

Ara,

$$\prod_{p\neq q}(-1,-abc)_p = \prod_{p\neq q}(a,b)_p \prod_{p\neq q}(a,c)_p \prod_{p\neq q}(b,c)_p.$$

Per la fórmula del producte (2.2.1) sabem que

$$\prod_{p\neq q}(-1,-abc)_p = (-1,-abc)_q, \quad \prod_{p\neq q}(a,b)_p = (a,b)_q,$$

$$\prod_{p\neq q}(a,c)_p = (a,c)_q, \quad \prod_{p\neq q}(b,c)_p = (b,c)_q.$$

Per tant,

$$(-1,-abc)_q = (a,b)_q(a,c)_q(b,c)_q.$$

I el resultat se segueix del teorema de Hasse-Minkowski. □

Teorema 3.4.5. *Si U i V són espais vectorials quadràtics regulars. U és representat per V si, i només si, U_p és representat per V_p per a tot p.*

Demostració. Suposem que V representa $\alpha \in \mathbb{Q}^*$ en tots els localitzats p. Aleshores $\langle -\alpha\rangle \perp V$ és isotròpic en tot $\mathbb{Q}_p$, per tant és isotròpic en $\mathbb{Q}$ en conseqüència representa α en $\mathbb{Q}$. Per tant, V representa α sempre que ho faci en tots els localitzats. Això prova el teorema en el cas en què $\dim(U) = 1$. Fem inducció sobre $\dim(U)$. Sigui $\alpha \in Q(U)$, aleshores $\alpha_p \in Q(U_p) \subseteq Q(V_p)$. Per tant, α és representat per V_p en tot p, en conseqüència és representat per V, per tant, tenim

$$U = L \perp U', \quad V = K \perp V',$$

on $L \simeq \langle\alpha\rangle$ i $K \simeq \langle\alpha\rangle$. Pel teorema de Witt (3.1.11) tenim la representació $U_p \longrightarrow V_p$ i $U'_p \longrightarrow V'_p$ per a tot p. Per tant, $U' \longrightarrow V'$ per inducció i obtenim $U \longrightarrow V$. □

Teorema 3.4.6 (Hasse-Minkowski general)**.** *Si U i V són espais vectorials regulars sobre un cos global k. Aleshores, U és isomètric a V si, i només si, $U_\mathfrak{p}$ és isomètric a $V_\mathfrak{p}$ per a tot $\mathfrak{p}$.*

Demostració. Pel teorema anterior existeix una representació $U \longrightarrow V$. Donat que U és regular la representació és una isometria. □

Capítol 4

Contraexemples al principi de local-global.

En aquesta secció l'objectiu és mostrar que, en general, el principi local-global no és cert en un context general d'equacions homogènies i algunes altres.

4.1 El contraexemple de Selmer

Teorema 4.1.1. *L'equació* $3X^3 + 4Y^3 + 5Z^3 = 0$ *té solució no trivial en* $\mathbb{Q}_p$ *per a tot* p *primer, però no en té cap en* $\mathbb{Q}$.

Demostració. Demostrar l'existència de solucions en els cossos p-àdics és molt senzill. La demostració de que l'equació no té solucions racionals requereix un estudi més exhaustiu i resultats de teoria algebraica de nombres.

En primer lloc, veure que té solucions reals és trivial.

Si $p = 3$, prenem $x = 0$ i $z = -1$, d'on obtenim $4Y^3 - 5 = 0$, per tant provar que existeix solució és equivalent a veure que $5/4$ és un cub 3-àdic. Pel Lema de Hensel general (1.3.5), necessitem $\beta \in \mathbb{Z}_p^*$ tal que $|\beta^3 - 5/4|_3 < 1/9$, si agafem $\beta = 2$ funciona. Per tant, té solució.

Si $p = 5$ posem $x = 1, z = 0$ i obtenim $3 + 4y^3 = 0$, és a dir $y^3 = -3/4$, com que tot element de $\mathbb{F}_5^*$ és un cub i si $f(Y) = Y^3 + 3/4$, $f'(y) \not\equiv 0 \pmod 0$ per a tot $y \in \mathbb{F}_5^*$.

Ara, per a tot $p \neq 3, 5$, si 3 és un cub en $\mathbb{F}_p^*$ pel lema de Hensel (1.3.6) 3 és un cub en $\mathbb{Z}_p$ és a dir $x^3 = 3$ per a un $x \in \mathbb{Z}_p$ i tenim la solució $(x, 1, -1)$.

Si 3 no és un cub, el grup de cubs té índex 3 i $\mathbb{F}_p^*/\mathbb{F}_p^{*3} = \{1, 3, 9\}$. En efecte, $\mathbb{F}_p^*$ és un grup multiplicatiu cíclic. Sigui g un generador, aleshores g^3 és un generador de $\mathbb{F}_p^{*3}$.

Recordem que

$$o(g^3) = \frac{o(g)}{\mathrm{mcd}(3, o(g))}.$$

Per tant,

$$[\mathbb{F}_p^* : \mathbb{F}_p^{*3}] = \frac{o(g)}{o(g^3)} = \mathrm{mcd}(3, o(g)) = \mathrm{mcd}(3, p-1) \in \{1, 3\}.$$

I si $3 \notin \mathbb{F}_p^{*3}$ tenim que $[\mathbb{F}_p^* : \mathbb{F}_p^{*3}] = 3$, i $\mathbb{F}_p^*/\mathbb{F}_p^* 3 = \{1, 3, 9\}$.

De fet, podem observar que 3 és un cub si, i només si, $p \equiv 2 \pmod 3$ i no és un cub si $p \equiv 1 \pmod 3$.

Ara, argumentem per casos i recordem que $p \neq 3, 5$.

- Si $5 \equiv 1 \pmod{\mathbb{F}_p^{*3}}$ aleshores 5 és un cub mòdul p i en conseqüència p-àdic pel Lema de Hensel. I si, $y^3 = 5$ tenim la solució $(-y, y, -1)$.
- Si $5 \equiv 3 \pmod{\mathbb{F}_p^{*3}}$, $5/3$ és un cub p-àdic i si $x^3 = 5/3$ tenim la solució $(x, 0, -1)$.
- Si $5 \equiv 9 \pmod{\mathbb{F}_p^{*3}}$ 15 és un cub p-àdic, si $t^3 = 15$ tenim la solució $(3t/7, 5/7, -1)$.

D'aquesta manera hem vist que l'equació té solució no nul·la per a tot p-àdic. Vegem ara que no en té en $\mathbb{Q}$.

Suposem que té una solució (x_0, y_0, z_0) no nul·la tal que $3x_0^3 + 4y_0^3 + 5z_0^3 = 0$. Multipliquem l'equació per 2 i obtenim $(2y_0)^3 + 6x_0^3 + 10z_0^3 = 0$. Per tant, $(x, y, z) := (2y_0, x_0, -z_0)$ és tal que

$$x^3 + 6y^3 = 10z^3.$$

Estudiem l'equació

$$X^3 - 6Y^3 = 10Z^3.$$

Si suposem que almenys una de les components de (x, y, z) no és zero, aleshores vegem que cap d'elles és zero. En efecte, si dos fossin zero, l'altra també ho seria. Si $x = 0$ tenim que $6y^3 = -10z^3$, com que suposem que ni y ni z són zero tenim que $6/10 = 3/5$ és un cub enter però això és fals. Si suposem $y = 0$ tenim que $x^3 = 10z^3$ com que suposem $x \neq 0 \neq z$ 10 hauria de ser un cub enter, cosa que no pot ser. Anàlogament amb $z = 0$, ja que 6 no és cap cub. Per tant, $xyz \neq 0$.

Podem suposar sense pèrdua de generalitat què

$$\mathrm{mcd}(x, y) = \mathrm{mcd}(x, z) = \mathrm{mcd}(y, z) = 1.$$

Si fem $x^3 = 10z^3 - 6y^3$ vegem que x és parell i, com que són dos a dos coprimers, y, z són senars.

Si fem $x^3 - 10z^3 = -6y^3$ vegem que $x^3 \equiv z^3 \pmod 3$, i com que si $3|x$ aleshores $3|z$ tenim que $3 \nmid x$ i $3 \nmid z$.

Si fem $x^3 - 6y^3 \equiv 10z^3$ obtenim que $x^3 \equiv y^3 \pmod 5$, argumentant igual, obtenim que $5 \nmid x$ i $5 \nmid y$.

Sigui ara $\alpha = \sqrt[3]{6}$. Factoritzem l'identitat anterior de manera que

$$(x + \alpha y)(x^2 - xy\alpha + y^2\alpha^2) = 10z^3.$$

El nostre objectiu és obtenir informació de l'aritmètica del cos $\mathbb{Q}(\alpha)$ i deduir resultats de la identitat anterior.

En primer lloc, vegem que $\mathbb{Z}[\alpha]$ és l'anell d'enters de $\mathbb{Q}(\alpha)$. El discriminant $\operatorname{disc}(\mathbb{Z}[\alpha]) = -27\alpha^2 = -3^5 \cdot 2^2$. Ara, el polinomi que defineix $\mathbb{Z}[\alpha]$ és $T^3 - 6$ que és 2-Eisenstein i 3-Eisenstein, per tant, l'índex de $\mathbb{Z}[\alpha]$ dins l'anell d'enters no és divisible ni per 2 ni per 3, en conseqüència és 1.

Passem ara aquesta igualtat a una identitat d'ideals principals en $\mathbb{Z}[\alpha]$.

$$(x + \alpha y)(x^2 - xy\alpha + y^2\alpha^2) = (10)(z)^3.$$

Factoritzem l'ideal (10) per obtenir informació sobre l'ideal $(x+\alpha y)$. Recordem que p factoritza en $\mathbb{Z}[\alpha]$ tal com $T^3 - 6$ factoritza en $\mathbb{F}_p$ (cf. [4]). Aleshores, $T^3 - 6 \equiv T^3 \pmod 2$ i per tant, $2 = \mathfrak{p}_2^3$ i $T^3 - 6 \equiv (T-1)(T^2+T+1) \pmod 5$, d'on $5 = \mathfrak{p}_5\mathfrak{p}_{25}$. Deduïm doncs que existeixen uns ideals únics de normes 2 i 5 tals que $(10) = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}$.

Observem ara que per a qualsevol enter k tenim que $N(\alpha+k) = k^3+6$, així $N(\alpha-1) = 5$ i $N(\alpha-2) = 2$ per tant, $\mathfrak{p}_2 = (\alpha-2)$ i $\mathfrak{p}_5 = (\alpha-1)$. En conseqüència, per a un cert ideal $\mathfrak{b}$ volem veure que

$$(x + \alpha y) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{b}^3 = (\alpha - 1)(\alpha - 2)\mathfrak{b}^3.$$

Sigui $\mathfrak{p}$ un primer que divideixi $(x + \alpha y)$ i $(x^2 - xy\alpha + \alpha^2y^2)$, aleshores

$$x + \alpha y \equiv 0 \pmod{\mathfrak{p}}, \quad x^2 - \alpha xy + \alpha^2y^2 \equiv 0 \pmod{\mathfrak{p}}.$$

Però

$$x^2 - \alpha xy + \alpha^2y^2 = (x + \alpha y)^2 - 3xy\alpha.$$

Se segueix que

$$3xy\alpha \equiv 0 \pmod{\mathfrak{p}}.$$

Fem per casos

1. Si $\mathfrak{p}|3$ tenim que $N(\mathfrak{p}) = 3^k$ per a un k enter no nul, però $\mathfrak{p}|(z)^3$, per tant, $3|z$ que no pot ser perquè hem deduït abans que $3 \nmid z$.

2. Si $\mathfrak{p}|(x)$ aleshores, $x + y\alpha \equiv y\alpha \equiv 0 \pmod{\mathfrak{p}}$ és a dir, $\mathfrak{p}|(y)(\alpha)$, però x, y són coprimers, per tant $\mathfrak{p}|\alpha$.

3. Si $\mathfrak{p}|(y)$ tenim que $x+y\alpha \equiv x \equiv 0 \pmod{\mathfrak{p}}$ i per tant, $\mathfrak{p}|(x)$ que no pot ser, perquè de nou x i y són coprimers.

De manera que el factor que divideixi a $(x+y\alpha)$ i $(x^2-\alpha xy+\alpha^2y^2)$ ha de ser factor de (α) també, però no de (3). Ara $\alpha^3 = 6$ per tant, $(\alpha)^3 = (2)(3)$ i $\mathfrak{p}|(2) = \mathfrak{p}_2^3$ d'on se segueix, $\mathfrak{p} = \mathfrak{p}_2$. És a dir, tot factor dels ideals de l'esquerra de l'equació és una potència de $\mathfrak{p}_2$.

Com que x és parell, y és senar i α és divisible per $\mathfrak{p}_2$ només una vegada, $(x+\alpha y)$ només és divisible per $\mathfrak{p}_2$ una vegada. D'on se segueix

$$(x+\alpha y) = \mathfrak{p}_2\mathfrak{c}, \quad (x^2-\alpha xy+\alpha^2y^2) = \mathfrak{p}_2\mathfrak{c}',$$

on $\mathfrak{c}, \mathfrak{c}'$ són ideals coprimers en $\mathbb{Z}[\alpha]$ i $\mathfrak{p}_2 \nmid \mathfrak{c}$. És clar doncs que $\mathfrak{p}_2$ és un factor de $\mathfrak{c}'$ i hem de veure si $\mathfrak{c}$ o $\mathfrak{c}'$ és divisible per $\mathfrak{p}_5$ o $\mathfrak{p}_{25}$.

De l'identitat $x^3+6y^3 = 10z^3$ deduïm que $x \equiv -y \pmod 5$, en efecte, si $t \not\equiv 2 \pmod 5$ tenim que $x^3 \equiv x \pmod 5$. Ara, si $x \equiv 2 \pmod 5$, aleshores $-2 \equiv x^3 \equiv -y^3 \pmod 5$, és a dir, $y^3 \equiv 2 \pmod 5$ que no té solució. Anàlogament per a $y \equiv 2 \pmod 5$. Ara obtenim, $x+y \equiv 0 \pmod{\mathfrak{p}_5}$, és a dir $\mathfrak{p}_5|(x+\alpha y)$. Si $\mathfrak{p}_{25}|(x+y\alpha)$, aleshores $(5)|(x+\alpha y)$ i 5 és un factor de $x+\alpha y$ en $\mathbb{Z}[\alpha]$, cosa que implica que 5 divideix x, y en $\mathbb{Z}$, però això és fals. Per tant, $\mathfrak{p}_{25}$ no és cap factor de $(x+\alpha y)$ i en conseqüència ho és de $(x^2-\alpha xy+\alpha^2y^2)$.

Sigui $\mathfrak{c} = \mathfrak{p}_5\mathfrak{m}$ i $\mathfrak{c}' = \mathfrak{p}_2\mathfrak{p}_{25}\mathfrak{m}'$, llavors

$$(x+\alpha y) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{m} \quad i \quad (x^2-xy\alpha+y^2\alpha^2) = \mathfrak{p}_2^2\mathfrak{p}_{25}\mathfrak{m}'.$$

Multiplicant-los obtenim que $(10)\mathfrak{m}\mathfrak{m}' = (10)(z)^3$, i com que $\mathfrak{m}$ i $\mathfrak{m}'$ són coprimers, deduïm que $\mathfrak{m}$ i $\mathfrak{m}'$ són cubs. Com volíem veure.

Fent servir la igualtat que hem deduït obtenim que

$$\mathfrak{p}_2^2\mathfrak{c}\mathfrak{c}' = (10)(z)^3 = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}.$$

Volem ara informació dels ideals que ens queden indeterminats. Vegem que $\mathbb{Z}[\alpha]$ és un domini d'ideals principals tot fent servir la fita de Minkowski pel nombre de classes:

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{\operatorname{disc}(\mathbb{Z}[\alpha])} = \frac{16\sqrt{3}}{\pi} \approx 8.82.$$

Per tant, el grup de classes d'ideals de $\mathbb{Z}[\alpha]$ està generat pels ideals de norma igual o més petita que 8. Ja hem vist que existeixen ideals únics i principals que fan factoritzar (2) i (5). Ara, $T^3 - 6 \equiv T^3 \pmod 3$ per tant, $(3) = \mathfrak{p}_3^3$ i, com que $N(\alpha) = 6$ obtenim que $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$ que implica que $\mathfrak{p}_3$ és principal.

L'últim cas és (7) i $T^3 - 6 \equiv (T+1)(T-3)(T+2) \pmod 7$ per tant, $(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$ i tenim que $N(\alpha+1) = 7$, $N(\alpha+2) = 14$, $N(\alpha+4) = 70$. Com que $1, 2, 4$ no són de la mateixa classe mòdul 7 podem escollir com els factors. Per tant, $(\alpha+1) = \mathfrak{p}_7$, $(\alpha+2) = \mathfrak{p}_7'\mathfrak{p}_2$ i $(\alpha+4) = \mathfrak{p}_7''\mathfrak{p}_2\mathfrak{p}_5$ d'on deduïm que són ideals primers. Del que se segueix que el nombre de classes és 1.

Hem vist doncs que $\mathbb{Z}[\alpha]$ és un DIP, en conseqüència l'ideal $\mathfrak{b}$ és principal. Posem $\mathfrak{b} = (\beta)$ i obtenim

$$x + \alpha y = (\alpha - 1)(\alpha - 2)\beta^3 u$$

per a alguna unitat u que està unívocament determinada llevat de multiplicació per unitat cúbica.

Per a determinar les unitats mòduls les unitats que són un cub considerem el següent: $r_1 = r_2 = 1$ (el nombre d'immersions en un cos real i complex respectivament), per tant, $\mathbb{Z}[\alpha]^* = \pm\varepsilon^{\mathbb{Z}}$ i en conseqüència $\mathbb{Z}[\alpha]^*/(\mathbb{Z}[\alpha]^*)^3$ és cíclic d'ordre 3. Sabem també que $(2) = \mathfrak{p}_2^3 = (\alpha - 2)^3$, per tant,

$$\frac{(\alpha-2)^3}{2} = 1 - 6\alpha + 3\alpha^2$$

és una unitat. Ara, volem veure que no és cap cub, per a això fem servir el cos residual $\mathbb{Z}[\alpha]/\mathfrak{p}_7 \simeq \mathbb{F}_7$.

$$1 - 6\alpha + 3\alpha^2 = 1 - 6(-1) + 3(-1)^2 \simeq 1 + 6 + 3 = 3 \pmod{\mathfrak{p}_7},$$

que no és un cub, ja que no ho és en $\mathbb{F}_7$. Per tant, genera el grup de les unitats mòdul el de les unitats cúbiques.

Finalment, en la identitat $x + \alpha y = (\alpha - 1)(\alpha - 2)\beta^3 u$, podem escriure u com

$$u = \left(\frac{(2-\alpha)^3}{2}\right)^k v^3 = \frac{((2-\alpha)^k v)^3}{2^k},$$

on $v \in \mathbb{Z}[\alpha]^*$ i $k = 0, 1o2$. Multiplicant per 2^k en ambdós costats de l'equació podem agrupar $((2-\alpha)^k v)^3$ dins de β^3 i obtenim

$$2^k x + 2^k y\alpha = (\alpha - 2)(\alpha - 1)\gamma^3,$$

on $\gamma \in \mathbb{Z}[\alpha]$. Siguin $A, B, C \in \mathbb{Z}$ no tots nuls tals que $\gamma = A + B\alpha + C\alpha^2$, podem desenvolupar $(\alpha-2)(\alpha-1)\gamma^3$ com a combinació $\mathbb{Z}$-lineal de $1, \alpha, \alpha^2$ i igualem el factor de α^2 a zero. Obtenim

$$0 = A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6AC^2 + 6B^2C) + 6(AB^2 + A^2C + 6BC^2).$$

Clarament tenim que $3|A$, per tant $0 \equiv 6B^3 \pmod 9$ per tant, $3|B$, i d'aquí se segueix que $0 \equiv 36C^3 \pmod{27}$, és a dir, $3|C$. L'equació és homogènia de grau 3 en A, B, C, per tant podem eliminar un factor de $3^3 = 27$ per obtenir una identitat anàloga. Però pel principi del descens infinit, això no pot ser, i per tant tenim que $(A, B, C) = (0, 0, 0)$ que és una contradicció. Com volíem veure. □

4.2 Sistemes quadràtics i quàrtiques.

En aquesta secció veurem que els sistemes quadràtics i les quàrtiques estan íntimament relacionats en uns casos especials.

Siguin $a, b, c, d \in \mathbb{Z}$ tals que $b^2 - 4ac \neq 0$, a, c, d no nuls i d lliure de quadrats. Considerem el sistema

$$\begin{cases} aU^2 - bV^2 + cW^2 = dZ^2 \\ UW = V^2 \end{cases}. \tag{4.1}$$

Considerem també l'equació

$$aX^4 + bX^2Y^2 - cY^4 = dZ^2. \tag{4.2}$$

Lema 4.2.1. *El sistema 4.1 té solució no nul·la sobre $\mathbb{Z}$ si, i només si en té 4.2 una de no nul·la.*

Anàlogament, sigui p un primer. El sistema 4.1 té solució primitiva mòdul p^k si, i només si en té una de primitiva la quàrtica 4.2 i $k \geq 2$.

Demostració. Demostrem la primera part. Sigui (x_0, y_0, z_0) una solució de 4.2, aleshores $(x_0^2, x_0y_0, y_0^2, z_0)$ és una solució no nul·la de 4.1. Anàlogament, sigui (u_0, v_0, w_0, z_0) una solució no nul·la de 4.1, aleshores (v_0, w_0, z_0w_0) és una solució no nul·la de 4.2.

Provem la segona part. Si (x_0, y_0, z_0) és solució de 4.2 i és primitiva, aleshores clarament $(x_0^2, x_0y_0, y_0^2, z_0)$ és solució primitiva de 4.1.

Ara, si (u_0, v_0, w_0, z_0) és solució primitiva de 4.1, tenim que (v_0, w_0, z_0w_0) i (u_0, v_0, z_0u_0) són solucions de 4.2, si u_0, v_0, w_0 no són invertibles tenim que z_0 és invertible mòdul p^k amb $k \geq 2$, i per tant, d és divisible per p^k, però això no pot ser perquè d és lliure de quadrats. Per tant, al menys un de u_0, v_0, w_0 és invertible. Com volíem veure. Si $p \nmid d$ el resultat és cert amb $k = 1$. □

Lema 4.2.2. *Sigui k un cos i siguin $a, b \in k^*$. Siguin $x_0, y_0 \in k$ tals que $ax_0^2 + by_0^2 = 1$. En $k[T]$ definim*

$$q_1(T) = bx_0T^2 - 2by_0T - ax_0, \quad q_2(T) = -by_0T^2 - 2ax_0T + ay_0, \quad q_3(T) = bT^2 + a.$$

Aleshores, $aq_1^2 + bq_2^2 = q_3^2$ i almenys dos d'aquests polinomis són de grau igual a 2. A més a més, si la característica del cos no és 2, cap d'ells és associat a cap altre.

Demostració. La comprovació de que $aq_1^2 + bq_2^2 = q_3^2$ és clara. Com que $b \neq 0$ és clar que $\deg(q_3) = 2$ i de l'equació $aq_1^2 + bq_2^2 = q_3$ és necessari que $\deg(q_1) = 2$ o $\deg(q_2) = 2$.

Si la característica no és 2, tenim que x_0 i y_0 no cap d'ells no pot ser zero i cap dels q_i és zero. Si suposem que dos dels q_i són associats, de l'equació $aq_1^2 + bq_2^2 = q_3^2$ es té que els tres són associats i per tant q_1, q_2 serien constants multiplicades per q_3 ja que hauran de tenir grau exactament 2 ambdós. Però q_1 o q_2 té terme lineal, el que és una contradicció. □

Lema 4.2.3. *Sigui p un nombre primer, i $a, b \in \mathbb{F}_p^*$. Aleshores, existeixen $x_0, y_0 \in \mathbb{F}_p$ tals que $ax_0^2 + by_0^2 = 1$.*

Demostració. Si $p = 2$ aleshores prenem $x_0 = 1$ i $y_0 = 0$. Si $p > 2$ sigui $f(X) = b^{-1}(1 - aX^2)$, volem resoldre $Y^2 = f(X)$. Suposem que l'equació no té solució, aleshores el símbol de Legendre sobre p de $f(X)$ és -1 sobre p per a tot $x \in \mathbb{F}_p$. Pel criteri d'Euler, que diu que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

tenim que $f(x)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ per a tot $x \in \mathbb{F}_p$. Però això vol dir que el polinomi $f(X)^{\frac{p-1}{2}} + 1$ té p arrels, i el seu grau és com a màxim $p - 1$. Això és una contradicció, d'on se segueix el resultat. □

Lema 4.2.4. *Sigui p un primer. Si $f, g \in \mathbb{F}_p[X]$ de grau com a màxim 2 i són tals que per a tot $t \in \mathbb{F}_p$ tenim que*

$$\left(\frac{f(t)}{p}\right) = \left(\frac{g(t)}{p}\right),$$

aleshores f i g són associats. Anàlogament, si per a tot $t \in \mathbb{F}_p$

$$\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right),$$

f, g són associats.

Demostració. Vegem el primer cas. Pel criteri d'Euler,

$$\left(\frac{f(t)}{p}\right) \equiv f(t)^{\frac{p-1}{2}} \pmod{p}, \quad \left(\frac{g(t)}{p}\right) \equiv g(t)^{\frac{p-1}{2}} \pmod{p}.$$

Per tant, el polinomi $f(T)^{\frac{p-1}{2}} - g(T)^{\frac{p-1}{2}}$ és idènticament zero, ja que té p arrels i el seu grau és més petit o igual que $p - 1$. Per tant, $f(T)^{\frac{p-1}{2}} = g(T)^{\frac{p-1}{2}}$. I com que $\mathbb{F}_p[T]$ és DFU, tenim que f i g són associats.

Vegem ara el segon cas. Suposem que per a tot $t \in \mathbb{F}_p^*$

$$\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right).$$

Suposem que $p \neq 2$. Sigui $r \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}$, aleshores $\left(\frac{r}{p}\right) = -1$, per tant,

$$\left(\frac{f(t)}{p}\right) = \left(\frac{r}{p}\right)\left(\frac{g(t)}{p}\right) = \left(\frac{rg(t)}{p}\right),$$

per a tot $t \in \mathbb{F}_p$. Pel primer apartat, f i rg són associats. Però $r \in \mathbb{F}_p^*$, és a dir, f i g són associats.

Observem que si $p = 2$, $\mathbb{F}_2^* \setminus \mathbb{F}_2^{*2} = \varnothing$, però, per a tot $x \in \mathbb{F}_2^*$ el símbol de Legendre és 1 i segon cas és el primer, per tant ja ha sigut demostrat. □

Proposició 4.2.5. *Sigui p un primer senar i siguin $a, b \in \mathbb{F}_p^*$. Aleshores,*

$$aX^4 + bY^4 = Z^2$$

té solució en $\mathbb{F}_p$.

Demostració. Pel lema 4.2.3 existeixen $x_0, y_0 \in \mathbb{F}_p$ tals que $ax_0^2 + by_0^2 = 1$. Pel lema 4.2.2 existeixen $q_1, q_2, q_3 \in \mathbb{F}_p[T]$ tals que $aq_1^2 + bq_2^2 = q_3^2$. A més a més, com que $p \neq 2$ q_1 i q_2 no són associats, per tant, pel lema anterior, existeix $t \in \mathbb{F}_p$ tal que

$$\left(\frac{q_1(t)}{p}\right) \neq -\left(\frac{q_2(t)}{p}\right).$$

És a dir,

$$\left(\frac{q_1(t)q_2(t)}{p}\right) \neq -1.$$

Equivalentment, existeix $c \in \mathbb{F}_p^*$ tal que $c^2 = q_1(t)q_2(t)$, en particular almenys un d'aquests dos polinomis és no nul en t. Si $q_1(t) \neq 0$ tenim que $(q_1(t), c, q_1(t)q_3(t))$ és solució del sistema.

Si $q_2(t) \neq 0$ aleshores $(c, q_2(t), q_2(t)q_3(t))$ és solució del sistema. □

Proposició 4.2.6. *Sigui p un primer senar, i a, c, d nombres enters tals que p no els divideix. Aleshores, l'equació*

$$aX^4 + cY^4 = dZ^2$$

té solució primitiva mòdul p^k per a tot $k \geq 1$.

Demostració. Com que $p \nmid d$ tenim que $p^k \nmid d$ per a tot $k \geq 1$ i d té invers mòdul p^k. Posem en $(\mathbb{Z}/p^k\mathbb{Z})[X, Y, Z]$

$$d^{-1}aX^4 + d^{-1}xY^4 = Z^2.$$

Per la proposició 4.2.5 tenim una solució mòdul p (x_1, y_1, z_1). Si $z_1 \not\equiv 0 \pmod{p}$ aleshores, considerem $N = d^{-1}(ax_1^2 + cy_1^2)$, el polinomi $Z^2 - N$ té solució mòdul p. I, com que $z_1 \not\equiv 0 \pmod{p}$ i $p \neq 2$ és clar que $2z_1 \not\equiv 0 \pmod{p}$. Pel lema de Hensel tenim solució z_k mòdul p^k per a tot $k \geq 1$. I la nostra equació té solució (x_1, y_1, z_k). En particular, per a tot $k \geq 1$ existeix un natural n tal que $N \equiv n^2 \pmod{p^k}$.

Si $x_1 \not\equiv 0 \pmod{p}$, sigui x_1^{-1} el seu invers mòdul p^k. Aleshores tenim la solució $(1, y_1x_1^{-1}, nx_1^{-2})$. Si $x_1 \equiv 0 \pmod{p}$ tenim la solució $(x_1y_1^{-1}, 1, ny_1^{-2})$.

□

Teorema 4.2.7. *Sigui q un nombre primer tal que $q \equiv 1 \pmod{16}$. Sigui d un nombre enter lliure de quadrats tal que $\left(\frac{d}{q}\right) = 1$ (en particular $q \nmid d$), i tal que per a tot $p|d$, si $p \neq 2$, aleshores $q \in \mathbb{F}_p^4$. Aleshores, el sistema*

$$\begin{cases} U^2 - qW^2 = dZ^2 \\ UW = V^2 \end{cases} \tag{4.3}$$

té solucions primitives mòdul p^k per a tot p primer i per a tot $k \geq 1$ i té solucions reals. És a dir, el sistema 4.3 té solucions primitives p-àdiques per a tot p.

Observació 4.2.8. *Observem que el sistema 4.3 és un cas especial del sistema 4.1 amb $a = 1, b = 0, c = -q$.*

Demostració. L'existència de solució real és clara, per exemple $(q^{1/2}, q^{1/4}, 1, 0)$ és solució.

Trobar solucions mòdul p^k del sistema és equivalent a trobar-ne de l'equació $X^4 - qY^4 = dZ^2$.

Argumentem per casos.

- Si $p \nmid 2dq$ tenim que per la proposició 4.2.6 el sistema té solució primitiva mòdul p^k per a tot $k \geq 1$.
- Si $p = q$, aleshores sabem que $d \in \mathbb{F}_q^{*2}$. Per tant, $X^2 - d$ té solució x mòdul q, a més $x \in \mathbb{F}_q^*$, per tant, $2x \not\equiv 0 \pmod{q}$ ja que $2 \nmid q$. Pel lema de Hensel, per a tot $k \geq 1$ existeix un natural n tal que $n^2 - d \equiv 0 \pmod{q^k}$. I tenim la solució $(1, 0, n^{-1})$.
- Si $p|d$ senar, tenim que q és una potència quarta en $\mathbb{F}_p$, és a dir, existeix x tal que $x^4 - q \equiv 0 \pmod{p}$ i en particular $x \not\equiv 0 \pmod{p}$ ja que $p \nmid q$. Així $4x^3 \not\equiv 0 \pmod{p}$ i pel lema de Hensel per a tot $k \geq 1$ existeix n natural tal que $n^4 - q \equiv 0 \pmod{p^k}$. Aleshores tenim la solució $(n, 1, 0)$.
- Si $p = 2$, sabem que $q \equiv 1 \pmod{2^4}$. En particular, $q \equiv 1 \pmod{2^k}$ per a tot $k \leq 4$. Necessitem a natural tal que $|a^4 - q|_2 < 1/4$, és clar que existeix, i fent servir de nou el lema de Hensel obtenim el resultat.

□

Proposició 4.2.9. *Sigui d un enter lliure de quadrats, q un nombre primer que no el divideixi i tal que $q \equiv 1 \pmod{8}$. Si*

$$X^4 - qY^4 = dZ^2$$

té solucions enteres no trivials, aleshores, existeix un enter c tal que $c^4 \equiv d \pmod{q}$.

Demostració. En primer lloc si (x_0, y_0, z_0) és una solució podem trobar una solució (x_1, y_1, z_1) tal que són coprimers dos a dos. Si p divideix a dos de x_0, y_0, z_0, aleshores p divideix l'altre. En particular $p|x_0$ i $p^2|qy_0^4$ i com que q és primer $p|y_0$, per tant, $p^4|dz_0^2$ i com que d és lliure de quadrats tenim que $p^2|z_0$. Repetim el procés amb $x_0/p, y_0/p, z_0/p^2$ fins que siguin dos a dos coprimers.

Ara, sigui (x_1, y_1, z_1) una solució així. Sigui $p|z_1$, aleshores, $p \nmid x_1$ i $p \nmid y_1$. Per tant, $x_1, y_1 \not\equiv 0 \pmod{p}$. I de la congruència

$$x_1^4 - qy_1^4 \equiv 0 \pmod{p},$$

obtenim que $\left(\frac{q}{p}\right) = 1$, i per la llei de reciprocitat quadràtica $\left(\frac{p}{q}\right) = 1$. A més a més, $q \equiv 1 \pmod{8}$ per tant,

$$\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = 1.$$

D'aquí se segueix que z_1 és producte de residus quadràtics mòdul q. I ara, obtenim que

$$x_1^4 \equiv dz_1^2 \pmod{q},$$

és a dir,

$$d \equiv z_1^{-2} x_1^4 \pmod{q}.$$

Com que z_1 és un residu quadràtic, z_1^{-2} és una potència quarta mòdul q i també d.

□

Teorema 4.2.10. *Sigui q un nombre primer tal que $q \equiv 1 \pmod{16}$, sigui d un nombre enter lliure de quadrats tal que $\left(\frac{d}{q}\right) = 1$ (en particular $q \nmid d$) però $d \notin \mathbb{F}_p^{*4}$, i tal que per a tot $p|d$, si $p \neq 2$, aleshores $q \in \mathbb{F}_p^4$. Llavors, el sistema*

$$\begin{cases} U^2 - qW^2 = dZ^2 \\ UW = V^2 \end{cases}$$

no verifica el principi de Hasse.

Equivalentment, tampoc el verifica l'equació

$$X^4 - qY^4 = dZ^2.$$

Aquest teorema se segueix clarament dels resultats previs de la secció.

Proposició 4.2.11. *El sistema*

$$\begin{cases} U^2 - 17W^2 = 2Z^2, \\ UW = V^2. \end{cases}$$

no verifica el principi de Hasse. Equivalentment per a

$$X^4 - 17Y^4 = 2Z^2.$$

4.3 Productes de quadràtiques

Tractem ara un cas senzill en $\mathbb{Q}[X,Y]$. Farem una generalització a partir del següent exemple.

Teorema 4.3.1. *L'equació* $(X^2-2Y^2)(X^2-17Y^2)(X^2-34Y^2)=0$ *té solució en tot p-àdic, però no en té cap en* $\mathbb{Q}$.

Demostració. Fem $Y=1$. Vegem que en té en $\mathbb{Q}_2$. $17\equiv 1 \pmod 8$, així $1^2-17\equiv 0 \pmod{2^k}$, si $k=1,2,3$. Ara, l'ordre de la derivada és 1 i pel lema de Hensel X^2-17 té solució en $\mathbb{Z}_2$. Anàlogament, X^2-2 té solució en $\mathbb{Q}_{17}$ ja que $6^2-2\equiv 0 \pmod{17}$ i $2\cdot 6\equiv 12\not\equiv 0 \pmod{17}$. Pel Lema de Hensel tenim el resultat. Ara, si $p\notin\{2,17\}$ el producte dels símbols de Legendre

$$\left(\frac{2}{p}\right)\left(\frac{17}{p}\right)\left(\frac{34}{p}\right)=\left(\frac{34^2}{p}\right)=1.$$

En particular almenys un d'ells és igual a 1 i per tant, podem aplicar el Lema de Hensel un cop més. El cas $p=\infty$ és trivial.

Inversament, cap dels polinomis $X^2-2Y^2, X^2-17Y^2, X^2-34Y^2$ té solució no nul·la en $\mathbb{Q}$. Per tant, aquesta equació no satisfà el principi de Hasse.

□

De fet, aquest exemple pot ser generalitzat.

Teorema 4.3.2. *Sigui p un nombre primer senar tal que* $p\equiv 1 \pmod 8$. *Aleshores, l'equació*

$$(X^2-2Y^2)(X^2-pY^2)(X^2-2pY^2)=0$$

contradiu el principi de Hasse.

Demostració. Que no té solucions en $\mathbb{Q}$ és clar. Vegem les solucions locals.

El cas real és trivial. Vegem que en té en $\mathbb{Q}_2$, això és clar de que $p\equiv 1 \pmod 8$.

En $\mathbb{Q}_p$ en té ja que

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=1.$$

I apliquem el lema de Hensel (1.3.6).

El cas l primer diferent de 2 i p és fa mitjançant la identitat

$$\left(\frac{2}{l}\right)\left(\frac{p}{l}\right)\left(\frac{2p}{l}\right)=\left(\frac{(2p)^2}{l}\right)=1,$$

i aplicant el lema de Hensel (1.3.6). □

Teorema 4.3.3. *Siguin p, q dos nombres primers senars diferents tals que $p \not\equiv 3 \pmod 4$ i $q \not\equiv 3 \pmod 4$. Aleshores, l'equació*

$$(X^2 - pY^2)(X^2 - qY^2)(X^2 - pqY^2) = 0$$

contradiu el principi de Hasse.

4.4 Corbes de Fermat

Definició 4.4.1. *Sigui $p \geq 3$ un nombre primer. Una corba de Fermat C a coeficients en $\mathbb{Q}$ d'exponent p es defineix mitjançant l'equació*

$$aX^p + bY^p + cZ^p = 0,$$

on a, b, c són enters no nuls.

L'interès que desperten aquestes equacions en l'estudi dels contraexemples que hom pot donar al principi de Hasse són evidents.

L'objectiu d'aquesta secció no és doncs fer una exposició formal dels resultats, sinó exposar resultats rellevants i recents.

Teorema 4.4.2. *Siguin b i c nombres enters lliures de potències p-èssimes. Posem $\theta = c^{1/p}$, sigui $K = \mathbb{Q}(\theta)$, $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, posem $e = e(K)$ l'exponent del grup de classes de K i sigui $r \equiv e \pmod p$ amb $0 \leq r < p$, i $U(K)$ el grup d'unitats de K. Suposem que se satisfan les propietats següents:*

1. *Es té que $p^2 \nmid c$ i $c^{p-1} \not\equiv 1 \pmod{p^2}$. Equivalentment, $p \nmid f$.*
2. *Per a tot divisor $\mathfrak{b}$ de b, sigui β un generador fixat de $\mathfrak{b}^e$. Per a tot $\varepsilon \in U(K)$ mòdul potències p-èssimes, sigui $\varepsilon\beta = \sum_{0 \leq j < p} b_j \theta^j$ amb $b_j \in \mathbb{Q}$, i sigui $P(X)$ el polinomi $P(X) = \sum_{0 \leq j < p} f b_j X^j$. Suposem que per a tot parell $(\mathfrak{b}, \varepsilon)$, o bé existeix j tal que $r < j < p$ amb $\operatorname{ord}_p(b_j) = 0$, o bé existeix k tal que $0 \leq k \leq r - 2$ amb $\operatorname{ord}_p(\operatorname{disc}(P^{(k)}(X))) = 0$.*

Aleshores, l'equació $x^p + by^p + cz^p = 0$ no té solucions racionals no trivials.

D'aquest teorema se segueix ràpidament que hem de buscar les equacions que tenen solució per a tot p-àdic que compleixen les condicions del teorema. H. Cohen en [4] computa mitjançant PARI i aquesta és una llista de contraexemples trobats.

Corol·lari 4.4.3. *Les equacions $x^p + by^p + cz^p = 0$ tenen solucions no trivials en tot p-àdic però no en $\mathbb{Q}$:*

1. *Si* $p = 3$ *i* $b \leq c \leq 22$*, si, i només si,* $(b,c) = (3,20),(3,22),(4,15),(5,12),(6,10),(6,17),(10,15),(10,22),(11,15),(11,20),(12,17),(15,17),(15,20),(15,22),(17,20)$ *o* $(17,22)$.

2. *Si* $p = 5$ *i* $b \leq c \leq 12$*, si, i només si,* $(b,c) = (2,9),(2,10),(3,7),(3,10),(4,7),(5,7),(5,12),(6,10),(7,10)$ *o* $(7,12)$.

3. *Si* $p = 7$ *i* $b \leq c \leq 12$*, si, i només si,* $(b,c) = (2,5),(2,7),(3,6),(3,10),(4,9),(5,7),(6,11),(7,9),(7,10),$ *o* $(7,12)$.

4. *Si* $p = 11$ *i* $b \leq c \leq 22$*, si, i només si,* $(b,c) = (2,21),(2,22),(3,19),(3,21),(3,22),(5,17),(9,22),(10,22),(15,22)$ *o* (19.22).

Definició 4.4.4. *Dues corbes a coeficients en* $\mathbb{Q}$ *són* $\mathbb{Q}$*-isomorfes si existeix una aplicació bijectiva que transforma els punts racionals d'una corba en els punts de l'altra.*

Observació 4.4.5. *En el cas* $p = 3$ *i* $(b,c) = (6,10)$ *és el contraexemple de Selmer. Efectivament, hem vist a la demostració del teorema 4.1.1 que les equacions*

$$3X^3 + 4Y^3 + 5Z^3 = 0,$$

i

$$X^3 + 6Y^3 + 10Z^3 = 0$$

són $\mathbb{Q}$*-isomorfes.*

A més a més, els resultats presentats per Cohen en [4] i Kraus [9] semblen indicar que el següent resultat pot ser cert.

Conjectura 4.4.6. *Per a tot primer* $p \geq 3$*, existeixen infinites corbes de Fermat d'exponent* p*, dos a dos no* $\mathbb{Q}$*-isomorfes, que contradiuen el principi de Hasse.*

Aquesta conjectura apareix per primer cop en [8]. Ara ja sabem que no podem traslladar el principi de Hasse a grau superior, però aquest resultat ens mesura, d'alguna manera, la quantitat d'equacions en grau qualsevol que no compleixen el principi de Hasse.

Conclusions

En aquest treball fem un estudi dels nombres p-àdics, objectes àmpliament utilitzats en Teoria de Nombres, i apliquem tots els resultats per a estudiar els espais quadràtics. Hem desenvolupat una teoria prou forta per a poder enunciar i demostrar el teorema principal d'aquest treball, és a dir, el teorema de Hasse-Minkowski.

El teorema de Hasse-Minkowski és resultat clàssic que tracta equacions diofantines homogènies de grau dos; això, de manera natural, ens ha portat a preguntar-nos què succeeix en grau superior, i en conseqüència, a fer una recerca bibliogràfica sobre els contraexemples existents. En aquest sentit, hem hagut de fer servir tota la maquinària de Teoria de Nombres algebraica per a poder fer una presentació rigorosa i, així, hem vist una de les motivacions a l'hora d'estudiar conceptes com les immersions, els anells d'enters i la ramificació.

Des d'un punt de vista general, hem pogut comprovar que l'estudi de les equacions diofantines presenta un desafiament majúscul quan el seu grau augmenta. Per esmentar alguns exemples coneguts podem dir que l'equació general en una variable no és resoluble per radicals quan el seu grau és igual o més gran que cinc. Un altre exemple són les solucions de l'equació de Fermat que es poden parametritzar en grau dos, però no n'hi ha de no trivials per a grau més gran. De manera paral·lela, hem vist en aquest treball que el principi de Hasse no és cert en general quan el grau de l'equació és més gran o igual que tres.

Finalment, aquesta recerca bibliogràfica ens mostra que fins i tot en temes que poden semblar tan tancats com és l'estudi dels espais quadràtics, i conseqüentment l'estudi del principi local-global, encara continua la recerca matemàtica a fi de desvetllar les estructures més amagades dels nombres. Es poden esmentar encara molts resultats que es coneixen, com per exemple que el teorema de Hasse és encara cert per a cossos globals o d'altres sobre el principi de Hasse i també conjectures, com la que hem vist a la última secció (4.4.6). En definitiva, hem trobat problemes oberts que de ben segur seguiran entre les nostres inquietuds durant molt de temps.

Bibliografia

[1] Aitken, W.; Lemmermeyer, F.: *Counterexemples to the Hasse Principle*, Amer. Math. Monthly, 118 (2011), nº7, 610-628.

[2] Atiyah, M.F.; MacDonald, I.G.: *Introduction to commutative algebra*, Reading (Mass.) : Addison-Wesley, 1969.

[3] Borevitch, Z. I.; Chafarevitch, I. R.: *Théorie des nombres.*, Gauthier-Villars, Paris, 1967.

[4] Cohen, H.:*Number Theory Volume I: Tools and Diophantine Equations*. Graduate Texts in Mathematics. Springer, New York, 2007. ISBN:978-0-387-49922-2.

[5] Conrad, K.: *Hensel's Lemma*, (Data de consulta: 13/03/2017, URL: http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/hensel.pdf), 2016.

[6] Conrad, K.: *Selmer's Example*, (Data de consulta: 29/05/2017, URL: http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/selmerexample.pdf), 2016.

[7] Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995. ISBN: 0-387-94268-8.

[8] Halberstadt, E.; Kraus, A.: *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. 548 (2002), 167-234.

[9] Kraus, A.: *Contre-exemples au principe de Hasse pour les courbes de Fermat*. Acta Arithmetica 174 (2016), 189-197.

[10] Mordell, L. J.: *Diophantine equations*, Academic Press Inc., London, 1970.

[11] O'Meara, O.T.: *Introduction to quadratic forms*, Springer-Verlag, Academic Press, Berlin-Götingen-Heildeberg, 1963.

[12] Robert, A.M.: *A Course in p-adic Analysis*, Springer-Verlag,New York, 2000. ISBN: 0-387-98669-3.

[13] Serre, J.-P.: *A course in Arithmetic*. Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1973. ISBN: 0-387-90040-3.